From Spectre to Spectrum
Effective Military Offensive Network Operations

Moore, Daniel

Awarding institution:
King's College London

King's College London – Department of War Studies

From Spectre to Spectrum

Effective Military Offensive Network Operations

A thesis presented in fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

In the subject of

WAR STUDIES

Daniel Moore

Student No. 1224743
Word Count: 99620

Daniel Moore is a PhD Candidate in the Department of War Studies at King's College London. He is a former Israeli military intelligence officer, has worked as a cybersecurity researcher with the Israeli government and as a cybercrime researcher in IBM, and is now a security principal in Accenture Security's threat intelligence practice.

ABSTRACT

Cyber-warfare is frequently discussed and rarely seen. Network incidents classified as warfare mostly fall below the required threshold, and instead are varying criminal acts or peacetime information operations. That we distinguish where cyber-warfare begins and ends is essential towards using it effectively. The spectre of cyberwar can and should be turned into a spectrum of military offensive network operations (MONOs). This thesis argues that the underlying characteristics of MONOs draw heavily on existing military thought, and that MONOs can be best employed by militaries by correctly categorising them. By exploring the idea of *intangible warfare* – conflict waged through non-physical means such as the information space and the electromagnetic spectrum - existing operational and strategic doctrine can be adapted rather than reinvented.

While MONOs are often discussed as a monolithic operational space, they can usefully be divided into *presence-based* and *event-based* operations. The former are strategic capabilities that begin with lengthy network intrusions and conclude with an offensive objective. The latter are directly-activated tactical tools that can be field-deployed by personnel to create localised effects immediately. This top-level distinction is abstract enough to be usable by military planners and researchers and specific enough to create two meaningful categories. Once defined, the two categories are applied against military thought to show how different MONOs can contribute to the overall military effort. Three chapters are then dedicated to an in-depth examination of MONO strategy demonstrated by the United States, Russia, and China. Each of the three exhibits a unique approach to intangible warfare stemming from differences in culture, resources, history, and circumstance. It thus becomes possible to observe the relative advantages and disadvantages of each military and how they stand to benefit by better employing MONOs.

CONTENTS

INTRODUCTION

THE ARGUMENT

Computing is an indispensable facet of modern military operations, but attacking computers has yet to deliver on the promise of revolutionizing warfare. Intelligence collection, command and control, guidance, and weapons platforms themselves are all aided by networks. Even as networks have become pivotal in enabling joint operations, the spectre of cyberwar – envisioning battles waged between and against networks - has yet to come to fruition; war remains innately kinetic. The twenty-first century accompanied the explosive rise of the cyber-warfare narrative, but its actual utility in warfare remains unclear. It is imperative to have strategic thought lead the use of technology rather than have technology create de-facto strategies. As such, this thesis will ask – *What limits military forces from realising the potential of cyber-warfare, and how could these limitations be mitigated?*

"I have given Cyber Command really its first wartime assignment… and we're seeing how it works out[1]", half-heartedly claimed former U.S. Secretary of Defense Ashton Carter in April 2016, referring to the use of offensive cyber operations against the Islamic State in Iraq. "Even a few years ago, it would not have occurred to a secretary of defense to say, 'let's get cyber in the game', but here we have real opportunities[2]", he added. It is such broadly ambitious claims that introduce confusion rather than clarity, as the contribution from "cyber" to the campaign against the Islamic State seemed murky. Practitioners and researchers immediately suspected hyperbole from Carter's overtures on military integration of cyber-offensives. How useful were the so-called "cyber bombs[3]" against the Islamic State?

Fast forward to eighteen months later. A now-retired Carter candidly admitted in a Belfer Center special report on the Islamic State campaign that he was "…largely disappointed in Cyber Command's effectiveness against ISIS. It never really produced any effective cyber weapons or techniques[4]." Tension arose from the ownership of such capabilities by intelligence agencies, principally the National Security Agency; "When CYBERCOM did produce something useful, the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection[5]." Finally, he lamented: "none of our agencies showed very well in the cyber fight[6]." The first declared US attempt at network warfighting was deemed a failure by the very individual that spearheaded it.

---

[1] Geoff Dyer, "US Launches Online Assault against Isis," *Financial Times*, April 6, 2016, https://www.ft.com/content/4d98edd0-fba5-11e5-b3f6-11d5706b613b.

[2] Dyer.

[3] David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times*, April 24, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[4] Ash Carter, "A Lasting Defeat: The Campaign to Destroy ISIS" (Cambridge, Mass: The Belfer Center, October 2017), 33.

[5] Carter, 33.

[6] Carter, 33.

In 2018, nations openly incorporate cyber-warfare into their military doctrine. The People's Republic of China and the United States – among many others - have declared doctrine, formed units and invested considerable funds towards conducting operations over and against networks. The United Kingdom recently acknowledged that it "…has conducted a major offensive cyber campaign against Daesh[7]." Chinese military doctrine highlights cyberspace as a significant new aspect of warfare, accompanying the internal rise of networked combat capabilities[8]. Russian forces have deployed offensive network capabilities against Ukrainian critical infrastructure by causing a limited power outage at a power station concurrent to a low-intensity kinetic campaign in Ukraine[9]. Nations are increasingly realising that the potential in targeting networks ranges from manipulating news organisations to crippling military hardware; the usefulness of network operations lies within a broad spectrum of possibilities. Yet cyber-warfare did not appear in a vacuum; it is rooted in military history, technological progress and the development of modern doctrine. Identifying and mapping how such capabilities can be made useful in warfare is thus the focus of this thesis.

Some network attacks push against the accepted boundaries of warfare. In 2017, a destructive strain of malware flimsily masquerading as ransomware spread virulently around the world, wiping devices and inflicting billions of pounds in damages to numerous organisations and corporations[10]. The sum global damage inflicted by NotPetya was unprecedented. Production and operations were affected in multiple industries as companies scrambled to reimage computers and restore lost data. The infection vector soon pointed to a small Ukrainian software company used locally to pay taxes[11], though others were later discovered. It was suspected that the original intent was to wreak digital havoc within Ukraine, yet it was eminently clear that the malware had escaped its original boundaries. Whether that was intentional or not remains uncertain.

NotPetya is now publicly attributed to the Russian military by the United States[12], United Kingdom[13], and others. This unusual attribution was conducted both publicly and to a startling level of specificity. The message sent was anything but subtle; this was a military operation sanctioned by the Russian government. Yet nuance is needed in order to identify what is the utility of attacks such as NotPetya, how they contribute to a strategic narrative, and whether they even fundamentally can be classified as warfare. As the models presented in this thesis will suggest, based on targeting, impact, identity of the attackers, the underlying goals and existing relationships between victim and attacker,

[7] Jeremy Fleming, "GCHQ Director's Speech at CYBERUK 2018" (April 12, 2018).

[8] The State Council Information Office, "China's Military Strategy" (2015).

[9] Robert M. Lee, "Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered," SANS Industrial Control Systems Security Blog, January 1, 2016, https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered.

[10] Cybereason, "Paying the Price of Destructive Cyber Attacks," 2017, 2, https://hi.cybereason.com/hubfs/Content%20PDFs/Paying-the-Price-of-Destructive-Cyber-Attacks.pdf?t=1505592823490.

[11] David Maynor et al., "The MeDoc Connection," *Cisco Talos* (blog), July 5, 2017, http://blog.talosintelligence.com/2017/07/the-medoc-connection.html.

[12] U.S. Press Secretary, "Statement from the Press Secretary," The White House, February 15, 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

[13] NCSC, "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack," UK National Cyber Security Centre, February 15, 2018, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

NotPetya can be viewed as an act of cyber-warfare against the Ukraine, but not against the collaterally affected nations[14].

Incidents against networks occur daily, in troves. The overwhelming majority of these attempted intrusions are no more than an exploratory probe for weaknesses, easily shrugged off by automated defences. Beyond those, many successful compromises occur, leading to an unprecedented aggregate loss of sensitive data. Fewer still seek not just to extract data but also influence it and the systems that host it, resulting in attacks. Only a sliver of intrusions are carried out under a military mandate, seeking to achieve political-strategic goals by way of network attacks. Often conflated with intelligence operations or criminal activity, this fragment of malicious network activity has distinct characteristics that are explored within this thesis.

The primary goal is therefore to address *how military offensive network operations (MONOs) optimally can contribute to battlefield success on all levels of operation*. Rather than discussing the spectre of cyberwar, the goal is to piece together the spectrum of cyber-warfare. Military doctrine is built on accrued experience and historical analysis that can contribute immensely towards crafting a modern joint cyber-warfighting approach; the introduction of cyber does not necessarily mean abandoning conventional wisdom. By examining the intersection of established military strategy, information security, and the technical characteristics of military-used technology, it is possible to construct practical models that both help determine what constitutes military cyber-attacks and how these could reliably be integrated into military strategy across all three key facets of warfighting; strategic, operational, and tactical. A combination of doctrinal, technical, and strategic analysis helps bridge the gap between established practice and the seemingly new circumstances of cyber-warfare.

Typologies already exist for offensive network activities. US doctrine divides by purpose; MONOs may disrupt, destroy, degrade, deny, or manipulate their targets[15]. This is a useful distinction when attempting to distinguish between potential impacts but less compelling as overarching categories for the operations themselves. Each of the potential five purposes may just be a different payload at the end of identical processes. Healey and Rattray suggested a dozen parameters with which to categorize offensive network operations, creating a granular framework that is best applied to individual cases[16]. When comparing strategic implementation of MONOs between nations at scale, the framework becomes more unwieldy. A simpler solution would offer simple, easily identifiable categories with impactful distinctions.

At its core, this thesis will argue that all MONOs can be usefully divided into two primary categories; tactical *event-based operations*, and strategic *presence-based operations*. This distinction helps divide between areas of responsibility in military forces and intelligence agencies, and between capabilities that can be designated as field-deployed weapons and those that would require high-

[14] The 5-step cyber-warfare assessment model will be detailed in the first chapter.

[15] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, 41.

[16] Gregory J. Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington D.C.: National Academic Press, 2010), 82–83.

echelon political approvals. The differences between the two categories manifest across the entire operational lifecycle, thereby serving as an instructive way of classifying offensive activities by practitioners and researchers alike.

The categorical division presented in the thesis helps prevent both over-simplification and over-complication of offensive network operations. The tendency to lump all network intrusions as "cyber" strips away crucial distinctions that then make clear analysis immensely difficult. Intelligence operations are not attacks and placing information operations alongside destructive malware leaves much to be desired. At the same time, while offensive network capabilities introduce numerous intricate variables and technological circumstances, these considerations must be abstracted to the level where researchers, strategists, and policy-makers can make sense of them with their existing toolsets.

Four layers will be introduced forming an analytical funnel for MONOs. The first layer will provide a five-step model towards assessing if a given incident should be classified as cyber-warfare. The model allows independently standardizing all assessment of offensive activities to the same scale, excluding those that do not meet a threshold of relevance. The second layer will then offer a historical analysis contending that MONOs draw heavily from existing warfighting doctrine, essentially grouping electronic warfare and network warfare in a century-long effort to conduct *intangible warfare*. The third layer will contend that distinguishing between immediate-effect *event-based operations* and time-consuming, clandestine *presence-based operations* can help form more coherent doctrine for each. The fourth and final layer will apply the above distinction to established military stratagems, showing how existing strategic thought can usefully apply to MONOs.

It is possible and desirable to disambiguate between military operations in wartime and information operations in peacetime. Hacks that manipulate a nation's elections process[17] may be an egregious violation of sovereignty, but do not necessarily meet the threshold of warfare. Unless carried out by military forces and for a commensurate conflict goal, shaping public perception by manipulating news and social media is not inherently an in-conflict venture. To give policy makers, strategists, doctrine-crafters, and battlefield commanders a robust understanding of what they can and cannot expect from offensive network operations, we must first dispel the "grey areas" currently afflicting such capabilities. While it is tempting to leave "cyber" as a porous concept where wartime and peacetime inherently bleed into each other, doing so introduces risk and waste. The risk entails undue escalation between nations as a result of misidentifying peacetime operations as ones of war-like intent[18]. Waste may stem from the misapplication of offensive network capabilities by strategists and battlefield commanders.

Cyber-warfare has the potential to provide a set of capabilities that act as a force multiplier in armed conflict, yet these will not supplant but rather complement existing warfighting doctrine.

---

[17] DHS Press Office, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," Department of Homeland Security, October 7, 2016, https://www.dhs.gov/node/23199.

[18] Ben Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017).

Uniquely, MONOs primarily allow attackers to weaponise an enemy against itself by subverting its systems, networks and weapons, thereby contributing to - but not single-handedly generating - victory. The more advanced and interconnected the adversary is, the more it may be susceptible to this form of operation. History instructs us about the many similarities between the advent of cyber-warfare and the introduction of other forms of warfare, specifically manoeuvres and tactics employed via the electromagnetic spectrum throughout the 20th century.

CONCEPTS

Clearly defined concepts are crucial to the scoping agenda at the heart of this thesis. An uncomfortable realisation is that information security professionals often skew negatively towards "cyber" as a term of art. In its most abstract, appending cyber as a prefix simply means "involving a computer". A reasonable concern is that as most human functions and interactions become more reliant on some form of computed involvement, the term itself becomes redundant. Yet for now, cyber is unavoidable. The term appears in policy documents, media coverage, Western military strategy, and official public reports. Irrespective of the sentiment towards it, cybersecurity is a meaningful concept because we ascribe it as such. As of now, using cyber as a linguistic qualifier effectively reflects the intersection of all other topics with networks and computing.

However, for the purpose of this thesis, "cyber" and "network" will be used nearly interchangeably. Both entail the use of interconnected computing resources, and thus effectively mean the same. Thus network-warfare and cyber-warfare are analogous, as are network attacks and cyber-attacks. This substitution is not particularly new; the National Security Agency has relied on the term "computer network operations" for several decades. To encourage robust application of concepts introduced through this work, use of the cyber prefix is often limited to where referencing existing terminology, titles, or organisations.

The concept most fundamental to this thesis is the military offensive network operation (MONO). For the purpose of this research, it shall be defined as *any means of digitally affecting adversary systems and networks for a military goal or objective*; affecting data by using data. This definition includes a wide swathe of possible offensive vectors while excluding non-offensive operations or kinetic operations against network equipment[19]. Most of what is characterized as network-warfare today is in fact routine intrusion operations conducted by intelligence agencies in peacetime. When espionage and corporate sabotage are intermixed with actual network attacks, it becomes increasingly difficult to distinguish what passes the threshold of warfare. If nations were to adopt the wider view of cyber-warfare that incorporates espionage, the escalatory ramifications for international diplomacy would be dire.

[19] Cyber-espionage and cyber-warfare routinely get fused together by media outlets and researchers, muddling the observable space.

In a 2015 Wall Street Journal article titled "Cyberwar Ignites a New Arms Race", the authors claimed that "more than two dozen nations have accumulated advanced cyberweapons in the last decade.[20]" While this may be true, the corroborating evidence in the piece was limited to espionage and wiping of corporate workstations. As targeting of corporate entities occurs frequently in peacetime, it is dangerous to repeatedly insinuate that the world is engulfed in constant unrelenting cyber-warfare. By itself, cyberwar is an awkward term attempting to depict a conflict through networks that is detached from other forms of political contest. As a result, this thesis will only briefly address cyberwar as a term of art and instead focus on a more integrative perception of cyber-warfare. To accurately frame what falls within the remit of cyber-warfare, a coherent depiction of offensive cyber capabilities is necessary in a manner that exceeds mere acts of espionage or localized sabotage. Cyber-warfare must be framed to generate proper boundaries and thresholds.

No widely accepted term currently exists to describe the evolution of forms of warfare that do not have a kinetic, physical manifestation. Jamming, electronic warfare, computer network operations, cyber-warfare, and information warfare all share several common characteristics: they rely on the unseen transmission and manipulation of data. As military forces become increasingly physically distant from the violence they inflict upon people and property, data conduits become significantly more meaningful to the conduct of war. Data affects communication, telemetry, coordination, targeting, command, intelligence, navigation, and planning. Striking at the channels which silently enable these functionalities is an understandably important undertaking, one that has commensurately evolved as they themselves have. The term offered by this thesis to encompass all efforts to undermine transmission, reception, and processing of data is *intangible warfare*. While it is a more descriptive rather than technical label, exploring how it practically evolved over the last eight decades will illustrate the continuity it embodies. Intangible warfare may differ in technique, approach or effect, but there is strong historical scaffolding that ties all such operations together; this will be explored throughout.

STRUCTURE

This thesis has two essential parts – the development of three core conceptual arguments, and their subsequent application to doctrine and use-cases. Conceptual work is meant to gradually disambiguate elements of MONOs that are often mischaracterised. Chapter one introduces a model to assess what constitutes cyber-warfare, chapter two examines how cyber organically grew out of other operational arts, and chapter three identifies the core categories within offensive network operations. These principles are then applied to modern warfighting doctrine in chapter four, and then subsequently tested against three case studies – US joint operations doctrine, the Russian use of network force in modern conflict, and a potential flaring of a Chinese-led Taiwan contingency. The

[20] Damian Paletta, Danny Yadron, and Jennifer Valentino-DeVries, "Cyberwar Ignites a New Arms Race," *Wall Street Journal*, October 12, 2015, sec. World, http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128.

final eighth chapter briefly examines how the provided models may be challenged by near-future trends.

Chapter one will argue that *most network intrusions today do not meet the threshold of an attack, and most attacks do not meet the threshold of warfare*. Put simply, a jarring majority of what is colloquially labelled cyber-warfare does not merit the label. To alleviate the classification challenge, the chapter will describe a detailed five-step process to qualify an incident as a cyber-warfare event. The steps accumulate and are increasingly difficult to meet. The five parameters inspected in order are; the affected target, the impact of the incident, the identity of the attacker(s), the goals behind the incident, and the existing relationship between victim and attacker. These five characteristics form to create the assessment model, made purposefully generic as to be applicable to a wide variety of malicious network incidents.

Chapter two will argue that *offensive network capabilities are a natural evolution of technological warfare*. In contrast to present US doctrine[21], "cyber" does not have to stand as a distinct warfighting domain; networks wholly permeate the existing physical domains. William Lynn, former U.S. Deputy Secretary of Defense stated already in 2010 that "…the Pentagon has formally recognized cyberspace as a new domain of warfare[22]." He then continued to explain that "although cyberspace is a man-made domain, it has become critical to military operations." The perspective that networks are a novel, distinct domain of warfare with previously unseen characteristics is a loaded one. It is possible to challenge this perspective both by observing how cyber-warfare came to be and it is potentially and practically employed. Offensive capabilities are developing in a world where increasingly complex warfighting platforms breed increasingly digitized countermeasures. Tanks gave birth to anti-tank weapons; warplanes necessitated the advent of radars and anti-aircraft platforms. Active radars rapidly led to electromagnetic countermeasures. Commensurately, the rise of thickly networked, informationised warfare is now giving birth to offensive network operations. Some elements may be novel but the discipline is not devoid of context; eight decades of counter-innovation warfare birthed network operations.

Within the historic analysis, the development of increasingly intangible forms of warfighting will be grouped under the term *intangible warfare*. As the historical analysis will show, most elements that exist within modern network warfare are borrowed from other operational arts. It is an evolutionary rather than revolutionary advancement; intangible warfare has existed for decades and had simply evolved as technology progressed and networking permeated both life and warfare. Existing characteristics of intangible warfare have rapidly exasperated to the point where they appear revolutionary. From the need to hide abilities lest they be compromised to the debilitating dependency on accurate intelligence, cyber shares key commonalities with electronic warfare that should not be

[21] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," May 2, 2013, 3-12.
[22] William Lynn, "Defending a New Domain - The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (October 2010): 101.

ignored. Shared characteristics can in turn help understand how existing doctrine can instruct on better use of network operations.

Chapter three will offer a doctrinal model in which *offensive network military operations will primarily fall into one of two categories; event-based, and presence-based*. While the former describes near-instantaneous effects achieved over and against networks, the latter entails all operations which include purposeful, lingering manoeuvring within adversary networks in order to plant and eventually activate offensive capabilities against targeted systems. Event-based attacks are thus roughly similar to classic weapons, and more suitable for deployment by battlefield commanders and individual warfighters. Presence-based attacks must include breaching adversary networks in advance – often by intelligence organisations – and are carefully activated by senior decision-makers[23] as to properly incorporate the risks involved in doing so. Differences between presence-based and event-based operations are explored by an in-depth examination through the prism of the US Department of Defense's Common Cyber Threat Framework[24]. The framework details the network operation life-cycle by splitting it into four principal phases; preparation, engagement, presence, and effect.

Demarcating between event and presence-based lends organic clarity to analysing offensive network operations. The two categories are so distinct that grouping them together causes a dilution of any attempt to operationalise network warfare. Operational considerations, technical limitations, personnel requirements and most importantly – the potential contribution, are so disparate between event and presence-based operations that it becomes nearly meaningless to observe them together. By separating them so, evaluating the utility, purpose and role of offensive military network operations becomes more feasible. The distinction also allows easier allocation of resources and can help alleviate issues where nation-state intelligence agencies indiscriminately hoard capabilities for fear of losing precious access to adversary sources.

Chapter four then argues that *event-based operations are largely effective militarily on the tactical-operational level, while presence-based attacks are primarily useful to facilitate operational-strategic effects*. The application of such operations to the conduct of war is explored by analysing military strategy across military history, applying relevant observations to offensive network operations. Clausewitz, Liddell Hart, Corbett, Freedman, and others all contribute valuable lessons on how technology can reshape the conduct of warfare, but not fundamentally alter its nature. Military strategy draws on millennia of accumulated wisdom. While it is tempting to infer that the man-made nature of the internet alters the underlying calculus of war somehow, it yet remains a contest of political will embodied through the application of coercive violence. Cyber-warfare may upset existing symmetries and enable creative manoeuvres, but utilising it correctly requires understanding where it

[23] For example in official U.S. cyber-warfare doctrine, only the Secretary of Defense and the President can authorise such operations. See U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities," February 12, 2014, 38.

[24] U.S. DNI, "A Common Cyber Threat Framework: A Foundation for Communication" (Office of the Direction of National Intelligence, 2013), https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf.

has the most utility. This can be done by dissecting technical characteristics and cross-referencing them with stratagems.

Event-based attacks will most commonly have a localised effect, thus limiting their utility to the tactical or at most the operational levels of warfare. This parameter is offset by their generic reusability; they are intended to be repeatedly employable against various targets and are more difficult to defend against. Whether it is destructive malware which will wipe computers and servers[25], a denial of service capability that prevents access to a vital communication network, or even a plane-mounted exploit against an aging air defense radar[26], these capabilities are intended to provide battlefield support, erode specific adversary assets and interrupt local decision-making.

Presence-based attacks may manifest as deep target network intrusions with effects extending into the strategic level. Sabotaging logistics may result in military assets incorrectly resourced away. Disrupting military satellites may adversely affect communications and GPS service across a theatre. By their nature, however, strategic attacks are highly specialised, require extended periods of preparation, research, and maintaining access to protected adversary networks. In many cases, potential targets of presence-based attacks are also valuable intelligence assets; such considerations must be accounted for at the highest echelons prior to deployment. In some cases, a presence-based capability may be a one-off chance at inflicting strategic harm; it is therefore best saved for when crucially needed.

Chapters five, six, and seven then endeavour to apply the entire theoretical scaffolding to different case studies. Models are best tested against disparate examples, embodying nations that have wildly different approaches to offensive network operations. Analysing how American, Russian and Chinese militaries can and do operate against adversary networks tests the offered models and highlights the unique advantages and disadvantages that each military has. The US has vast technical capabilities, the Russians have prolific, aggressive use of full spectrum MONOs, and the Chinese have developed a cogent yet largely untested doctrine.

Chapter five will dive into the US approach to cyber as a distinct domain of warfighting. Since the late twentieth century, the US has de-facto developed a broad array of potent technical capabilities meant to target networks and devices. Publicly, significant slivers have been made available through leaks, public sector research, government doctrine, and technical data from the sprawling defence industry. Yet much like in the earlier days of modern warfare, the US adopted a capability-first approach, which resulted in numerous potential MONOs that were mismatched with available doctrine. As a result, battlefield successes were reportedly limited, with presence-based offensives relegated to a war-prevention role and event-based capabilities limited to supporting special forces and operations. With its global rivals increasingly adopting the same principles of highly-networked

[25] Ryan Faughnder, Dave Paresh, and Saba Hamedy, "Hack at Sony Pictures Shuts Computer System," *The Los Angeles Times*, November 24, 2014, http://www.latimes.com/entertainment/envelope/cotown/la-fi-sony-hack-20141125-story.html.

[26] Sean O'Conner, "Access Denial - Syria's Air Defence Network" (Jane's International Defence Review, 2014).

joint operations, the US could effectively employ MONOs to enhance its existing asymmetries and deny adversaries their own.

Chapter six will examine Russian military network activity. Since 2007, Russia has increasingly exerted coercive will against other nation-states. In a desire to occlude the appearance of actual war, Russian doctrine heavily favours deploying semi-clandestine forces and low-visibility capabilities. As a result, conflicts involving Russian forces or interests exhibit numerous references to offensive network operations, ranging from degrading fighter aircraft[27] to direct attacks against critical infrastructure[28]. Where the United States has created a separate unified combatant command to oversee "cyber operations", the Russians engage with offensive network capabilities holistically in a spectrum that blurs distinction between peacetime and wartime, and between information operations and network warfare. Russian doctrine borrows heavily from well-established Soviet principles of reflexive control – the desire to covertly shape adversary behaviour to a more favourable pattern. While Russia is incredibly prolific in its employment of offensive network behaviour, the vast majority of its operations do not merit being labelled as warfare. This will be shown to be intentional and in line with Russian aims; by consistently remaining below the threshold of all-out war, their leadership can avoid a military response from capable adversaries.

Chapter seven will explore the evolving Chinese doctrine to network operations, particularly through the prism of a potential conflict with Taiwan. This possibility is neither remote nor entirely theoretical; several previous crises have already occurred, and both external assessment and internal doctrine envision the two parties on a collision course which will eventually require resolution. The scenario pits three highly networked militaries – China, Taiwan, and the United States - all seeking swift resolution of hostilities. As a result, such a conflict is a prime case study for the potential employment of offensive network capabilities in order to prevent effective command and control, and degrade networked warfighters from achieving objectives. China has undertaken great strides to modernise its approach to MONOs, including the concentration of capabilities in a new independent Strategic Support Force meant to provide capabilities to the existing domains. Yet, as with other aspects of the People's Liberation Army the doctrine remains largely untested under conditions of conflict, with a dearth of operational expertise a crucial deficiency in achieving superiority in MONOs.

The final eighth chapter will draw conclusions based on all tiers of analysis. The conclusions include the culmination of efforts to fuse historical, technical and military perspectives towards a cohesive examination of cyber-warfare. The underlying arguments will be shown to indicate that despite the rapid pace of advancement, militaries worldwide can adopt conceptual tenets of cyberwarfare that would then aid in its battlefield deployment. On a foundational level, it is useful to decouple information operations from network warfare. The lessons of electronic warfare can similarly allow militaries to accommodate network forces without altering doctrine too heavily.

---

[27] Marco Giannangeli, "Russians 'Hacking into' RAF Crews over Syria," *The Daily Express*, January 15, 2017, http://www.express.co.uk/news/world/754236/russia-raf-bombers-syria-hacking-missions-military-army.

[28] Dragos, "CRASHOVERRIDE: Threat to the Electric Grid Operations" (Dragos, June 12, 2017).

Finally, the distinction between combatants carrying out presence and event-based operations can help resolve organisational tensions and vastly different operational lifecycles.

This thesis attempts to map the utility of cyber-warfare and place it within a wider military context. While we yet lack more of the desired observable evidence, we by no means are without the tools to assess the shape of digital warfare. If an informed strategic debate is meshed with a practical technical analysis, the resulting amalgamation is a realistic assessment of the characteristics of cyber-warfare. The existing lack of clarity manifests in overstatements and alarmism; countering it yields boundaries, advantages and possibilities.

Methodology And Sourcing

Direct evidence of military engagements against networks is relatively lacking, but an interleaved pattern of different sources creates a tapestry of complementary information. *This work relies on critical assessment of sources across four axes; technical, operational, doctrinal, and strategic.* Until history provides a richer offering of case studies to examine, those seeking to understand network operations must rely on cautiously informed assessments based on existing evidence.

The technical axis entails an examination of how networks and devices may be targeted for effect. Put simply, some effects are either infeasible or unrealistic to carry out. Whereas disabling a tactical communication network is both possible and plausible, causing a nuclear submarine reactor to undergo a critical failure is a far more remote possibility due to existing failsafes and mitigation procedures. Expectation alignment is a key part of a thesis that seeks to chart what warfare may realistically look like when carried out through and against networks. Technical assessment is carried out by inspecting the specifications of military equipment and networks and the potential vulnerabilities that these may be afflicted with. Examples to this include difficulty due to the overreliance on aging, hard-to-update technology, or the increasing tendency to introduce remote command and control directly into weapons.

Sourcing on technical specification of military hardware and software includes freely available manuals on military standards, officially published reports, leaked sensitive data, and even promotional materials published by military contractors entrusted with designing and manufacturing military equipment. US government accountability reports shine a fascinating light on assessed vulnerabilities and limitations of newly developed warfighting platforms. Combined, a fairly robust mesh of military-deployed technologies emerged supporting an analysis of how these may be targeted in wartime.

An example of covering emerging technologies from complementary angles is the F-35 Lightning II Joint Strike Fighter. This ambitious project includes numerous contractors and participating nations spanning over a decade of research and development. By design, the project is meant to both integrate well into existing orders of battle, while simultaneously offering state-of-the-art sensors, onboard software, and peripheral logistics and maintenance systems. Sources on the F-35 platform include

official accountability reports detailing software flaws[29], public coverage on recurring errors on the F-35[30], official specifications of the F-35's "ALIS" semi-autonomous logistics system[31], and even leaked classified documents pertaining to BYZANTINE HADES[32], the network operation in which crucial intelligence pertaining to the F-35 project was exfiltrated - presumably by Chinese threat actors. By and large, the F-35 exhibits deep flaws that may be exploited for effect by a determined adversary. Possible operations may include disruption of the onboard radar suite, interference in the next-generation communication protocols used by the craft, or even a lengthy presence-based operation to disrupt logistics and maintenance by corrupting regionally-deployed ALIS units. Such attack vectors are not merely theoretical when the plane itself exhibits numerous issues, and its own auditors express scepticism at the craft's software readiness for sustained operations in a contested airspace.

Network attacks are ubiquitous. There is no dearth of evidence when it comes to mapping a multitude of techniques for targeting networks and devices. The unprecedented public scrutiny of nation-state network intrusion tools meant an explosion of public-sphere analysis of offensive network operations and capabilities. These vary in quality and relevance, but uniquely provide a glimpse into how networks are targeted by nation states for effect. As the intelligence agencies behind network intelligence campaigns are often those that will precipitate network attacks, learning of their craft and methodology by dissecting analysing their intrusions is paramount. There are lessons to be learned from analysing they excel, make errors, and perhaps most importantly, how they adapt to challenges and evolve their capabilities[33]. Visibility into network operations spans numerous countries, threat actors, and underlying goals. In some cases, coverage of intelligence operations reveals complex, modular toolsets[34] that could be applied to a variety of offensive purposes should there be an inclination to do so. In other cases, reviewing how nations successfully degraded adversary systems hints at how similar operations may materialise against equivalent military targets. The toolsets apply to both generic event-based attacks and the most targeted and expansive of presence-based attacks.

Sourcing for network intrusion analysis extends beyond the information security industry. Several batches of leaked materials pertaining to compromised intelligence agencies provide intimate access to internal documentation and assessments of operational capabilities within some of the most capable network aggressors. Disclosures include the expansive Snowden documents leaked from numerous U.S. agencies and units including the National Security Agency (NSA) in 2013, the leak of

[29] See for example two reports from 2015- U.S. Department of Defense, "Fiscal Year 2015 DoD Programs - F-35 Joint Strike Fighter (JSF)" (U.S. Department of Defense, January 2016). and 2016 - U.S. Department of Defense, "Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF)" (U.S. Department of Defense, January 2017).

[30] Sean Gallagher, "F-35 Radar System Has Bug That Requires Hard Reboot in Flight," *Ars Technica*, March 10, 2016, https://arstechnica.com/information-technology/2016/03/f-35-radar-system-has-bug-that-requires-hard-reboot-in-flight/.

[31] Lockheed Martin, "Autonomic Logistics Information System (ALIS)" (Lockheed Martin, November 2009), https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/alis/CS00086-55%20(ALIS%20Product%20Card).pdf.

[32] U.S. Department of Defense, "Chinese Exfiltrate Sensitive Military Technology," 2011, http://www.spiegel.de/media/media-35687.pdf.

[33] See for example the evolution from Duqu to Duqu 2.0, malware families from 2011 and 2015 respectively, both ostensibly attributed to Israel. GReAT, "The Duqu 2.0: Technical Details" (Kaspersky Lab, June 11, 2015), https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/.

[34] See for example the intrusion toolset known as APT, a highly modular platform used to compromise high value targets. GReAT, "The ProjectSauron APT" (Kaspersky Lab, August 9, 2016), https://securelist.com/faq-the-projectsauron-apt/75533/.

sensitive information from the NSA's Tailored Access Operations unit by a group calling itself "The Shadow Brokers" in 2016[35], and the leaks codenamed Vault-7 allegedly containing a vast repository of information on CIA intrusion and attack capabilities[36].

The doctrinal axis is evaluated by relying on official publications and de-facto nation-state behaviour. Most simply, nations often publicise their relationship with offensive network operations within their core official documents, such as national military strategies. The detail level of these documents varies greatly based on the country analysed, with the United States arguably engaged in the most significant public discourse around shaping its operational capabilities. However, in order to generically assess doctrinal elements to offensive network operations, documents, reports, and speeches from several key nations are addressed.

Nations vary greatly in their approaches to network warfare doctrine. Extensive US literature on the topic reveals an evolutionary approach which increasingly views "cyber" as an independent domain of warfare. If taken at face value, the new domain then requires distinct doctrine and allocation of resources. Evidence for this is most immediately reflected in Joint Publication 3-12 – Cyberspace Operations[37], which then has complementary implementations in branches such as the US Air Force[38] and the US Army[39]. Other documents, including manuals on joint operations[40] also shed light on how existing strategies could be updated to reflect the inclusion of novel capabilities. Other declassified documents similarly contribute complementary elements.

For other nations, some high-level documents allow identification of how policy makers and military strategists view the role of network operations. The evolution of official military doctrine from Russia[41] and China[42] are highly indicative of the role of network operations as capable of altering conventional asymmetries and creating unique advantages. Views of network warfare vary based on the overall perception of information and its role in conflict. This in turn affects how nations seek to weaponise information against their adversaries.

Official publications need not be the only doctrinal elements considered. As language expertise is lacking, academic coverage of regional publications provides invaluable access to strategic perspectives of network warfare within military-academic circles. Dedicated limited-distribution journals in Russia and China – most commonly written to by senior staff – reveal how those within their respective systems view offensive network operations. Russian doctrinal assessments from NATO's Cyber Centre of Excellence[43] or Project 2049's assessment of how a Chinese operation against

[35] The actual publication of materials was carried out by a group calling itself "The ShadowBrokers", suspected as a Russian false-flag information operation.

[36] As of this writing, The Vault leaks are hosted on WikiLeaks and can be found here - Wikileaks, "Vault 7: CIA Hacking Tools Revealed," Wikileaks, March 7, 2017, https://wikileaks.org/ciav7p1/.

[37] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018.

[38] U.S. Air Force, "Air Force Doctrine Document 3-12," July 15, 2010.

[39] U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities."

[40] U.S. Joint Chiefs of Staff, "Joint Publication 5-0: Joint Planning" (US Joint Chief of Staff, June 16, 2017).

[41] Russian Federation, "The Military Doctrine of the Russian Federation," December 25, 2014, http://rusemb.org.uk/press/2029.

[42] The State Council Information Office, China's Military Strategy.

[43] Keir Giles, NATO Defense College, and Research Division, *Handbook of Russian Information Warfare* (Rome, Italy: NATO Defence College Research Division, 2016).

Taiwan[44] may manifest are useful towards scoping a realistic set of potential offensive operations available to these nations.

The strategic axis includes the wealth of accumulated knowledge from two millennia of strategic thought. Since Thucydides first charted the course of the Peloponnesian Wars and Sun Tzu remarked on the value of subterfuge for warfare, military thinkers have grappled with the contribution of technology to warfare. Particularly with the dawn of machine warfare in the early twentieth century, the notion of technology permanently altering the nature of war itself has been pervasive yet contested. By looking for applicable lessons from military strategists and academics, it becomes possible to identify where opportunities for offensive network capabilities truly lie.

Several of cyber-warfare's core appeals and limitations can be dissected through the prism of historic strategists. In many cases, some elements appear to fit while others do not. Such for example with one of warfare's most oft-referenced figures, Prussian military theorist Carl von Clausewitz. Supposedly, the over-emphasised Clausewitzian focus on destruction as the key means of creating battlefield success hints at its inapplicability to network warfare, where most operations cannot create such an effect. At the same time, the gradual creation of networked nerve centres for command and control have effectively created new centres of gravity, which if struck successfully by a network attack could have a reverberating effect.

Other parallels exist. Liddell Hart's praise of indirect warfare[45] and Douhet's adherence to strategic bombing are both useful theoretical constructs through which we can assess the significance of offensive network operations. It is meaningful to examine whether MONOs can disrupt the balance of power by bypassing concentration of forces or enact coercive punishment. Perhaps, but history instructs that previous such attempts have largely been unsuccessful. Thus, we can avoid repeating the follies of previous new technologies by learning from their attempted integrations. Corbett's identification that strategy manifests differently in the maritime and land domains holds fascinating analogies to the so-called cyber domain. Modern cyber-warfare researchers such as Libicki[46], Denning[47], Rattray[48], and Healey[49] all have contributed analyses and conceptual frameworks that comment on the viability of such attack vectors.

LIMITATIONS

Research undertaken to explore military network operations immediately encounters two interconnected difficulties; capabilities are often highly classified, and evidence of use is scarce. These difficulties are not insurmountable, but merely complicate attempts at fashioning an inclusive

[44] Ian Easton, *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia*, 1st ed. (Arlington, Virgina: Project 2049 Institute, 2017).
[45] B.H. Liddell Hart, *Strategy*, 2nd rev. ed (New York, N.Y., U.S.A: Meridian, 1991).
[46] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).
[47] Dorothy E. Denning, *Information Warfare and Security*, 4th ed. (Reading: Addison-Wesley, 1999).
[48] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass: MIT Press, 2001).
[49] Rattray and Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use."

framework that would accurately reflect MONOs as they may be used. The diverse sourcing employed when dissecting such capabilities is the answer; assembling a mosaic of network warfare from disparate fragments of information reveals a rather compelling result. Available technical data informs about military equipment vulnerabilities. Leaked information and public-domain analysis of nation-state network operations instruct on the techniques and strategy used by nations. Strategic documents, official statements and academic analysis help fashion assessments on the potential use of MONOs to military campaigns.

The above approach does not fully alleviate the concern regarding the partiality of coverage. Considering the rapid pace of development in the field, commenting on modern capabilities may be difficult. However, that should not preclude the attempt. While technology evolves, most of its underpinnings have remained unchanged for the last five decades. The modern internet has inherited an architecture first developed in the 1960s[50]. Military equipment today must still support communication protocols first introduced in the 1970s. By design, military warfighting equipment is designed to last decades, with internal software and hardware gradually evolving over time. Thus, looking at the military network space reveals that much of it relies on technology incepted decades ago, now fully understood and accessible to researchers.

An intentional limitation imposed is wholly excluding broader information operations from the scope of analysis. As previously said, the impetus to doing so is clear; information operations cover an immense swathe of non-violent activities that muddle analysis of capabilities employed in warfare. While combat operations may certainly incorporate information warfare, and some nations such as Russia fuse them seamlessly with other facets of intangible warfare, they remain sufficiently distinct as to merit exclusion. Without excluding information operations from the analysis, attempting to scope where military responsibility lies becomes near-impossible. How can network warfare capabilities be relegated to battlefield commanders if the distinction between them and psychological operations is hazy? Rather than being a detriment, segmenting information operations to a separate frame of observation lends clarity to the ontologies offered in the thesis. Different frameworks exist to discuss information warfare.

A third limitation relates to future-proofing the argument and models offered in this thesis. With the rise of artificial intelligence and increased automation, it is unclear whether the considerations offered in this thesis will effectively persist. While this is always a concern when researching technology, it is especially so for network warfare which is intrinsically vulnerable to shifts in technological trends. However, this realisation does not necessarily impair the validity of the arguments offered.

Artificial intelligence represents a potential future reality in which military operators are further distanced from the decision-making process by relegating more responsibilities to software. It is at times heralded as the next great “game-changer”, an introduced element that will upset the existing

[50] See for example the ARPANET and the rise of packet-switch networking, the tenets of which remain applicable to date.

advantages and disadvantages of network operations. Supposedly, human operators seeking to target networks protected by artificial intelligence would struggle to bypass it's heightened situational awareness. However, while artificial intelligence signifies a meaningful leap in the predictability of doing so, it is in fact quite congruent with the existing trends. Once artificial intelligence becomes ubiquitous in defending network assets from man-made attacks, operators on the offensive side may naturally turn to such capabilities to devise counters[51]. In this sense, artificial intelligence may yet form the next step in a long-existing process, an escalation of trends that have begun with the radar wars of the Second World War.

[51] This process has already begun, as presented by a DARPA program for AI-based network defence, see Wade Shen, "The Information Domain and the Future of Conflict" (June 1, 2017).

1. A THEORY OF CYBER-WARFARE

OVERVIEW

How can warfare be waged with software? The practice of military combat evokes imagery of opposing forces colliding against each other in increasingly sophisticated ways. The spear, the horse and the shield gave way to the bow, the rifle and the missile. Throughout the ages, war has charted an evolutionary course in which the finest technology of the time was wielded to facilitate organised acts of violence. Efforts into maintaining an edge in the art of war had a tremendous effect on other walks of life. The same forge used to craft the blade was also used to craft the work tool. The same innovations in rocketry devised to fuel Cold War ballistic missiles were used to send humans into space. A tight-knit symbiosis formed between military technology and its civilian counterparts; one bred the other, the former fed the latter, and vice versa. The development of combat waged over networks – what is colloquially called cyber-warfare – is one iteration of that same cycle of innovation.

If this thesis strives to gauge the boundaries and roles of cyber-warfare, this chapter seeks to deconstruct the term into its component parts. The primary purpose of the chapter is an exercise in boundary-setting; an examination of what acts perpetrated through networks do and do not meet the threshold of network warfare. The contemporary environment is replete with network intrusions, ranging from exfiltration of information to tangible asset loss reaching millions of dollars and even physical damage. Where many of the tools of warfare are distinctly operated by militaries, the most influential intrusions have notably been perpetrated by intelligence agencies. Should they be assessed on the spectrum of intelligence operations or warfare?

The chapter will seek to answer these questions by offering five cumulative parameters with which network attacks can be individually assessed, those being *target, impact, attacker, goals* and *relationships*. Together, the parameters form a model that excludes most incidents which are out of scope for analysis of MONOs. Discerning that the affected targets (1) are of sufficient significance or quantity is the first milestone in identifying a warfare-threshold activity; a think tank does not equate to a military target. Impact (2) includes both the immediate observable effects of the attack and its wider consequences, as most public domain incidents have little or no physical effects on the afflicted party. Attributing the attacker (3) allows establishing affiliation or subordination to a state or sub-state entity overseeing the attacks. Goals (4) relate to assessing that the agenda of the perpetrators is military-strategic, crucial in an ecosystem where most intrusions are motivated by criminality or loose ideology. Finally, relationships (5) address the larger geopolitical and strategic considerations in which the attack takes place, and is often the key differentiator between warfare and other adversarial situations. All five parameters must be met if an incident is to qualify within the spectrum of cyber-warfare.

Standardised assessment based on the above five parameters can help discern an act of war from an intelligence campaign, or a criminal enterprise from a well-organised precursor to a military attack. These distinctions are often less trivial than it may seem in software-based attacks. In the wake of mass exfiltration of sensitive information and nation-sponsored attacks against the banking sector as occurred in the US[52], the most resonating question is often "what does this attack mean?" If the answer is the devolution of the political circumstance into war, it is far more consequential than an embarrassingly successful espionage campaign. Incidents that are below the model's threshold are thereafter considered out of scope when dissecting MONOs, and would only be addressed insofar as to demonstrate how nations often blur the lines between MONOs and other types of network operations.

The second process included in the chapter is disentangling cyber-warfare and cyberwar. While the former can be established as a distinct sub-element of generalised warfare, the latter holds little tangible value beyond colloquialism and theoretical debate on the instrumentality of war through networks. Cyberwar and cyber-warfare are often used interchangeably in publication and media to denote any friction between two parties over the internet; that lack of distinction can be harmful to the overall quality of the discussion. cyberwar does not inherently exist as a meaningful independent construct and may subsequently be replaced with the appropriate label based on the underlying context and motivation, be it crime, espionage or actual acts of war.

Similarly, although it is a thoroughly Western concept, a comprehensive framing of cyber-warfare must extend beyond the manner in which it is perceived by the United States. Awkward and misappropriated analogies have only detracted from generating agreed upon standards. The difficulties in crafting a cohesive ontology of MONOs was noted at least as early as 2001, when US Air Force veteran Gregory Rattray noted in his book, *Strategic Warfare in Cyberspace*, that "Frameworks for evaluating the capabilities of international actors to conduct conflicts based on attacking information infrastructures remain underdeveloped[53]". He continued to aptly warn that the label of information warfare was being too broadly applied.

This was exemplified in April 2016 when US deputy secretary of defence Robert Work colourfully exclaimed - "We are dropping cyberbombs[54]" when discussing the ongoing military campaign against the Islamic State. The particular phrasing drew sharp criticism from observers, but it served to reflect the military perception of the value of offensive network capabilities. At the same time, the Russian term for cyberwar – *kibervoyna* - mostly only exists as an acknowledgement of Western thinking rather than an actual centrepiece of Russian doctrine[55]. As a rising number of nations openly or tacitly acknowledge the significance of various offensive software capabilities to their strategy, cyber-warfare must appropriately expand as a concept to envelop its different manifestations. Concurrently,

---

[52] Ilan Berman, "The Iranian Cyber Threat, Revisited," § US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (2013), 2, http://www.china.usc.edu/sites/default/files/legacy/AppImages/house-2013-berman-cyber-threats.pdf.

[53] Rattray, *Strategic Warfare in Cyberspace*, 2.

[54] Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat."

[55] Keir Giles, "Russia's 'New' Tools for Confronting the West" (London, U.K.: Chatham House, March 2016), 9.

expanding the scope of MONOs risks dilution of analysis beyond utility. Striking a balance between inclusiveness and cohesion is thus at the core of this effort.

This chapter will explore numerous examples of malicious network activities that despite their elevated public profiles should not be depicted as warfare. In 2014, Sony Pictures was the victim of a destructive network attack that resulted in data loss, exfiltration of sensitive information, severe disruption in daily operations and many millions of US dollars in damages[56]. In a relatively rare act of public attribution, then FBI Director James Comey publicly pointed an accusatory finger at the attackers: "…we know who hacked Sony. It was the North Koreans who hacked Sony[57]". The offensive was widely indicated to be a continuation of North Korean policy by cyber means, a strike at the heart of the American studio that dared to publish the parody movie *The Interview*. The movie presented revered North Korean leader Kim Jong Un in a comical manner with the entire film centred on his attempted assassination. Public attribution efforts of the attack pointed to Unit 121 of the North Korean Reconnaissance General Bureau, one of the hermit nation's more notorious hacking units[58] often associated with offensive network activities[59]. By 2018, the US government had indicted an operative affiliated with the North Korean government for this attack and others[60]. In this sense, the Sony attack straddled the grey area between warfare and non-warfare activities, with its unique set of capabilities applicable to both. While the visible, high-profile attack held the possibility of escalation, it resulted in no apparent kinetic or virtual countermeasures save heated rhetoric. As the offered model will subsequently show, the Sony hack failed to meet multiple criteria necessary to qualify as a warfare-threshold incident.

The Boundaries of Cyber-Warfare

When the virtual medium itself is mostly intangible, communication of consensually agreeable limitations on the conduct of war becomes even more significant. The barrier of entry for conducting some forms of offensive action over the internet has decreased immensely; it is arguably easier to generate a noticeable effect against a military network than it is to physically affect a missile battery. In this sense, the global internet has provided both opportunity and capability, and has reduced the barrier of entry somewhat[61]. The novelty of modern networking entails that we must be able to distinguish between the various sub-categories of friction in cyberspace between two entities.

The delineation is crucial, as improperly establishing the boundaries of warfare can lead to peacetime operations being incorrectly classified as belligerent. In 2015, an intrusion into the US

---

[56] Peter Elkind, "Sony Pictures: Inside the Hack of the Century," *Fortune* (blog), July 1, 2015, http://fortune.com/sony-hack-part-1/.

[57] James B. Comey, "Addressing the Cyber Security Threat," Speech, Federal Bureau of Investigation, January 7, 2015, https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

[58] HP Security Research, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape" (Hewlett Packard, August 16, 2014).

[59] Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations" (Center for Strategic & International Studies, December 2015), 41.

[60] Nathan P. Shields, United States of America V. Park Jin Hyok, No. MJ 18-1479 (United States District Court June 8, 2018).

[61] To successfully affect operational military assets would still require a complete operational cycle and devotion of resources that are far beyond the capabilities of most non-state actors. See follow-up chapters for extensive elaboration on the unique calculus of MONOs.

Office of Personnel Management led to the exfiltration of sensitive personal information of over twenty million former and active members of the US security community[62]. Some Western political researchers such as Eurasia Group's president Ian Bremmer[63] were quick to tie the event into a large cyber-warfare narrative in which the US is in active contest with China. At the same time, the Chinese government attempted to diffuse the tensions from its hack by perceptibly collaborating with the US. It formally acknowledged the intrusion but labelled it an act of crime rather than a nation-state breach of sovereignty[64]. The distinction mattered even if the US did not fully accept the Chinese explanation; both parties had no desire to escalate, and the situation eventually diffused. Ascertaining why the OPM incident did not herald the onset of further hostilities can be made clearer by assessing each incident characteristic separately.

As indicated before, five characteristics have been chosen to distinguish warfare-level attacks to other offensive incidents, such as financially-motivated criminality or illegal ideological incidents. The parameters are *target, impact, attacker, goals and relationships*. They are not ordered by importance as all five parameters must be met, but rather by increasing difficulty of assessment. Put differently, while discerning the exact intended victim of an attack is often the easiest endeavour, surmising the significance of the underlying strategic and political relationship between attacker and target is the most daunting of tasks in the process. There is a gradual, steep increase in the complexity of analysis required to meet each subsequent parameter.

The proposed five-step model is an evolution of existing approaches. In a lengthy 2012 analysis of offensive network capabilities by Harvard researchers Noyes and Belk[65], they proposed an ontology observing three criteria; target, effect, and objective. The ontology is used to aptly note that "…it is clear that the current classifications of offensive network operations are overly broad…[66]". While a meaningful step forward, the proposed ontology stops short of offering a complete solution for effectively reducing the existing breadth of operations classified as offensive or warfare. Healey and Rattray offered their own model in 2010, detailing a model that offered six types of military cyber missions that can then be categorised based on twelve parameters[67]. This model served as a useful inspiration from which the chosen parameters were distilled, as the inordinate number of characteristics and categories can make a model cumbersome to repeatedly apply.

Incident response to network attacks is an incremental process in which forensic evidence is analysed and subsequently connected to additional collected data. The sequence of parameters commensurately reflects this same natural order of inference. Identifying the victim is the genesis of

---

[62] U.S. OPM, "Cybersecurity Resource Center," U.S. Office of Personnel Management, accessed September 2, 2016, https://www.opm.gov/cybersecurity/.

[63] Ian Bremmer, "These 5 Facts Explain the Threat of Cyber Warfare," *Time*, June 19, 2015, http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/.

[64] Song Miou, "First China-U.S. Cyber Security Ministerial Dialogue Yields Positive Outcomes," *Xinhua News*, December 2, 2015, http://news.xinhuanet.com/english/2015-12/02/c_134874733.htm.

[65] Robert Belk and Matthew Noyes, "On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy" (Cambridge, Mass: John F Kennedy School of Government, 2012), http://www.dtic.mil/docs/citations/ADA561817.

[66] Belk and Noyes, 5.

[67] Rattray and Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," 81–84.

any investigation. Once the exact target – or targets - have been identified, it becomes possible to deduce the incident's impact on it, by observing deviations from the target's steady-state. Based on the victim and the evidence of the attack itself, it then becomes plausible to attempt and identify the incident's instigator by way of a careful attribution process. Only if attribution has been reasonably successful can the observer gauge motivations and underlying goals. Finally, the pre-existing relationship between the target's owning nation and the aggressor can be coupled with the overarching context in which this relationship exists.

The first examined parameter is assessing the incident's affected *target*. Initiating the process with a victim assessment provides an early opportunity to classify the attack's underlying purpose. Attacks against military assets, infrastructure and logistics will clearly meet this threshold as they are immediately indicative of an adversarial relationship of which at least one party is the warfighting apparatus of a nation or a nation-like entity. Almost unerringly, safeguarding the multitude of military networks and systems is an internal military responsibility and where most resources and efforts are allocated. As indicated by the US Department of Defense (DoD) Cyber Strategy from 2015:

> *"…DoD must defend its own networks, systems and information. The Defense Department must be able to secure its own networks against attack and recover quickly if security measures fail… Network defense operations on DoD networks constitute the vast majority of DoD's operations in cyberspace*[68]*".*

Thus a direct attack targeting any military asset would result in a response cycle initiated by the military responders. The affected party may in turn - based on the nature of the attack and its assessed perpetrators - choose to respond in force.

Critical national infrastructure forms the second major category against which attacks will meet the required threshold of warfare. China[69], Russia[70], the United Kingdom[71] and the United States[72] have all separately acknowledged that attacks against networks associated with critical national infrastructure such as energy, banking and communication shall be considered as potentially indicative of an armed attack against the nation itself. Critical infrastructure has largely been defined similarly by different nations. To quote a 2013 Turkish strategy document, critical infrastructure includes those networks "…who host the information systems that can cause, [1] loss of lives, [2] large scale economic damage, [3] security vulnerabilities and disturbances of public order at the national level [if compromised][73]".

Two incidents are worth evaluating as contrasting examples of targets. The 2014 attacks by North Korea against Sony's networks, destructive as they may have been, are immediately disqualified as

[68] U.S. Department of Defense, "The Department of Defense Cyber Strategy" (2015), 4.
[69] The State Council Information Office, China's Military Strategy.
[70] Russian Federation, "The Military Doctrine of the Russian Federation."
[71] UK Cabinet Office and Cabinet Office, "The UK Cyber Security Strategy: Report on Progress and Forward Plans" (2014), 13.
[72] White House, "International Strategy for Cyberspace," May 6, 2011, 2.
[73] Turkish Government, "National Cyber Security Strategy and 2013-2014 Action Plan" (Turkey: Ministry of Transport, Maritime Affairs and Communications, 2013), 9.

being warfare due to the nature of Sony Pictures Entertainment as the victim entity; it is a wholly private multi-national corporation that serves no critical function in the various services it offers. Thus, it immediately becomes apparent that the high-profile nature of the attack does not grant the US military recourse over the hack. Conversely, the alleged US-Israeli campaign to inflict physical harm against the Iranian nuclear program could – solely based on targeting of the Natanz uranium enrichment facility[74] - be initially construed as a warfare-threshold target. Interestingly, that attacking Natanz risks escalation may explain why Stuxnet was waged painstakingly covertly[75]; the underlying desire may have been to avoid the risk of retaliation for choosing such a sensitive target.

Finally, a third option towards meeting the target parameter is replacing quality with quantity. Where an attack against Sony is insufficient on its own to merit an escalation cycle, a simultaneous attack against all major movie studios – Paramount, 20th Century Fox, Sony and others – may be interpreted as a fundamental attack against American soft power. Similarly, governments would be hard pressed to ignore simultaneous destructive attacks against thousands of targets of opportunity, even if they are relatively insignificant on their own. The actual quantity to qualify the target threshold can either be a meaningful enough percentage of the targeted industry, or conversely simply hundreds or more of consecutive targets.

A popular approach to measuring the type and quality of network attacks is by examining their *impact* rather than the actions themselves. Michael Schmitt, an international law expert that served as one of the key architects of the norm-setting Tallinn Manual, previously claimed that the breadth of armed attacks conducted through cyberspace includes all acts that generate consequences analogous to their kinetic equivalents[76]. In a reality bereft of empirical examples upon which to assess "cyber armed attacks", anchoring the discussion on existing guidelines is reasonable. The existing legal framework is also useful when seeking to tether cyber-warfare to the laws of armed conflict, as Schmitt and his Tallinn Manual associates originally attempted. However, the disparity in effects between digital attacks and kinetic ones is insurmountable. Most offensive network capabilities are not consequentially analogous to physical attacks and will usually not yield comparable results. Otherwise put, barring the most extreme cases, offensive network capabilities will not physically destroy or impair their targets.

Schmitt and the first Tallinn Manual reflected that a cyber-armed attack is "…any action that causes death or injury… to individuals or damage or destruction of objects[77]". Impact is thus a primary source of divergence between cyber-warfare and kinetic warfare. By shackling the comparison to the physical domain as the Tallinn manual does, the end result suffers by excluding whole categories of attacks. One such example, data disruption attacks, would be left out of the narrow definitions

[74] Ralph Langner, "Stuxnet - Dissecting a Cyberwarfare Weapon," *IEEE Security and Privacy* 9, no. 3 (June 2011): 49.
[75] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier" (Symantec, February 2011), 37.
[76] Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context," in *4th International Conference on Cyber Conflict* (IEEE, 2012), 288.
[77] Schmitt, 288.

requiring observable damage. By the same metric, crippling the defensive capabilities of an adversary with a software-only attack is not an action permitting escalatory recourse.

Legal scholars do not uniformly agree with the parallel to physicality, as do many policy makers. In 2010, US Colonel and operational law expert David Graham noted that some interpretations of the 1949 UN Geneva Convention indicate that a use of force is deemed an armed attack if it is of "sufficient scope, duration and intensity[78]". This perspective affords a wider range of offensive actions to be folded into the scope of an attack. Official United States policy seems to echo this with the claim that any significant attack against critical infrastructure - to include banks and key service providers - may constitute an attack for which retaliation is merited; a complete metric is still lacking however[79].

The importance of understanding the variance in possible impacts has been echoed by renowned international relations scholar Joseph Nye. In his remarks on the roles of "cyber-power", Nye contrasted between hard and soft-power manifestations of cyber-activities, differentiating but ultimately recognising the importance of both tangibly affecting networks while also manipulating real world network-dependent public processes[80]. In short, cyber-warfare capabilities may adversely affect military networks, and they may also impact the functionality of critical public services in a disruptive but ultimately non-destructive manner.

That the *attackers* are organs of a nation-state or at least state-affiliated is crucial; the identity of the perpetrators is significant for determining culpability and the available countermeasures. Put differently, if an individual or an organised crime unit performs a hack of sensitive military networks, it does not immediately qualify that the nation hosting the unaffiliated attackers is culpable and must be penalised directly. Some form of affiliation must be established, or at the very least provable negligence in pursuit and resolution efforts by the host nation's law enforcement agencies. Nations cannot conduct war against criminal organisations, nor can they against individuals. A state or meaningful political sub-state entity must be the responsible party to the attack before a warfare approach can be used to assess the incident. This requires reaching an acceptable threshold of high-level attacker attribution.

Attribution of an attacker to a politically acceptable degree is a well-known challenge in network intrusions. The People's Republic of China's government has long been indicated to rely on a corps of a loosely-affiliated "non-governmental forces" (民间力量), capable of being tasked with pursuing national intelligence requirements and even conduct networked attacks[81]. Comparably, Russian network attacks against Estonia in 2007 and Georgia in 2008 have both been publicly depicted as citizen participation in weaponised online protest rather than an organised Russian assault, despite

[78] David E. Graham, "Cyber Threats and the Law of War," *J. Nat'l Sec. L. & Pol'y* 4 (2010): 90, http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jnatselp4&section=10.

[79] Dustin Volz and Karen Friefeld, "U.S. Issues First Government Guide on Responding to Cyber Attacks," July 26, 2016, https://www.yahoo.com/tech/u-financial-sanctions-response-cyber-attacks-124106828.html.

[80] Joseph S. Nye, "Cyber Power" (DTIC Document, 2010), 5, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626.

[81] Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," *China Brief* 15, no. 8 (April 17, 2015): 3–7.

indications pointing to the alternative[82]. The plausible deniability baked into the internet's easily achieved relative anonymity makes high degrees of certainty difficult when performing attacker attribution. As passionately echoed by Russian doctrine, the confusion sown in the wake of a network attack is one of the prominent advantages of the medium[83].

Attributing attackers thus becomes an issue of reaching an acceptable level of confidence in their identity. As Rid and Buchanan illustrated when presenting their model; "attribution is what states make of it[84]". Accepting that there are no absolute certainties, nations can turn to several approaches towards making assessments; an accumulation of technical forensic evidence, known operational techniques of the adversaries, external intelligence sources, and political context. The combination of the above can and has previously resulted in public attributions. In 2010, The Obama administration publicly directed allegations at the Chinese government for possibly facilitating a series of cyber intrusions against major US tech corporations, including Google[85]. In 2016, The Ukrainian security services publicly indicated that the Russian government was to blame for the network attack against a local power station[86] that resulted in a brief period of service disruption[87]. Reaching acceptable levels of attribution in cyberspace is therefore possible, even if it is a challenging endeavour.

Goals determine attacker motivation, and motivation is pivotal to assessing an attack's significance and appropriate countermeasures. The consequences of a network attack are fundamentally different if it was intended to pilfer sensitive information, influence public opinion, or disable an air defence radar. The mere characterization of an attack as both emanating from a nation-state organ and being highly disruptive or even destructive does not automatically mean it should be decried as an act of war. Whether the perpetrator was conducting economic espionage or seeking to subvert the sovereignty of the afflicted nation, the distinction is crucial towards assessing the afflicted party's available set of countermeasures.

The ambiguity of network operations means that goals and intent are often difficult to assess[88]. Whether an intrusion is an attack or meant for intelligence collection may in some cases only become apparent once the intruder decides to activate a malicious payload – or instead does not. It is roughly analogous to observing a burglar entering a house and inspect the rooms, waiting for him to attack the sleeping residents – or simply leave with their jewellery and cash. As with forensic assessment of burglaries, intruders may be sloppy and leave some indicators as to their intent. To pursue the break-in analogy further, the burglar may had left a knife as he fled. Indeed, Buchanan has indicated that

[82] R. J. Deibert, R. Rohozinski, and M. Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43, no. 1 (February 1, 2012): 3–24, http://sdi.sagepub.com/cgi/doi/10.1177/0967010611431079.

[83] Giles, "Russia's 'New' Tools for Confronting the West," 36.

[84] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 7.

[85] Bobbie Johnson, "US Asks China to Explain Google Hacking Claims," *The Guardian*, January 13, 2010, sec. Technology, https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us.

[86] Security Service of Ukraine, "Russian Hackers Plan Energy Subversion in Ukraine," Ukrinform, December 28, 2015, http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html.

[87] SANS Industrial Control Systems and E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid" (Washington, DC, March 18, 2016), 1–3, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[88] Belk and Noyes, "On the Use of Offensive Cyber Capabilities," 11.

this very issue stands at the core of what he called the "cybersecurity dilemma"[89]. Nations may inadvertently be drawn into a cycle of escalation as a result of misinterpreted network intrusions.

A basic distinction required is for intelligence operations, namely the demarcation between extraction of information and destructive sabotage. As history instructs, espionage has been a mainstay of international relations for millennia, dating back to ancient Egypt[90]. While compromise during espionage operations is nationally embarrassing and dangerous to the operatives involved, it rarely results in escalation to the level of open hostilities. Mutual espionage between rivals and allies is unfortunate but ultimately desirable conduct. Successful spying may reduce the levels of uncertainty as to an adversary's capabilities, disposition and intent, potentially allowing observers to make more informed decisions[91].

This differentiation is crucial, as no international legal framework bars non-destructive surreptitious espionage between adversarial nations[92]. To wit, a spy extracting information – as successful as they may be – does not grant the afflicted nation any legal recourse in the international arena. If captured, the spy would undoubtedly face the ramifications of breaching domestic anti-espionage laws, but therein the complications conclude. Between the two nations, the implications of such an ordeal rest squarely on the existing nature of the relationship between them. Internationally, the treaties governing non-harmful espionage and intelligence gathering are underdeveloped and vague, even if they do recognise that spying constitutes a breach in the targeted nation's sovereignty[93].

A notable caveat exists for cases in which active network intelligence collection appears to be a prelude to an armed attack; such instances may be considered a threat of use of force on their own standing[94]. As an example, spy plane sorties intent on highlighting targets for a subsequent attack meet this standard and may trigger self-defence countermeasures. A spike in network intrusion attempts on tactical military networks, if intertwined with a reasonable threat context and existing heightened tensions, may similarly reach the threshold meriting self-defence. Such acts are sufficiently escalatory as to be on a spectrum of operations that may lead up to hostile engagement and war.

Destructive acts of espionage, often referred to as sabotage, are tricky to classify. As previously stated, all aspects of modern life are reliant upon networks and computers. Adversely subverting their normal operation in a purposeful act can incur heavy financial losses, loss of critical functionality and in rare cases even manifest as physical damage and loss of life. Yet not all such cases are created equal. Attacks designed to disturb the flow of data and restrict access to services occur frequently, even with nation-state sponsorship. At least publicly not a single one of the purported cases culminated in open hostilities between nations, unless the attacks already transpired in the context of an existing conflict.

---

[89] Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*.
[90] Terry Crowdy, *The Enemy Within: A History of Spies, Spymasters and Espionage* (Bloomsbury Publishing, 2011), 15.
[91] Roger D. Scott, "Territorially Intrusive Intelligence Collection and International Law," *The Air Force Law Review* 46 (1999): 223.
[92] Scott, 218.
[93] Craig Forcese, "Spies Without Borders: International Law and Intelligence Collection," *Journal of National Security Law and Policy* 5 (2011): 185.
[94] Forcese, 198–99.

Most directly, if an aggressor acts in pursuit of military objectives or to prevent the accomplishment of those by the target, that shall be meet the cyber-warfare threshold for the "goals" parameter. This subset of goals has the clear determination of being directly carried out by armed forces or subordinate groups in order to achieve military goals – whether within active combat or without. US Department of Defense Joint Publication 3-12 titled 'Cyberspace Operations' makes clear the boundaries in which the armed forces operate in cyberspace to this effect where it states:

> *"Commanders conduct cyberspace operations (CO) to retain freedom of maneuver in cyberspace, accomplish the joint force commander's (JFC's) objectives, deny freedom of action to adversaries, and enable other operational activities*[95]*."*

The viability of network capabilities as part of a military objective is not unique to Western doctrine. Although a single cohesive Russian doctrinal document cementing the definition of network warfare is lacking, abundant official and unofficial Russian texts separately relate to information as crucial to modern battlefield dominance. As several Russian military theorists have posited in the journal *Moscow Military Thought* in 2009:

> *"[The] main objectives will be to disorganize (disrupt) the functioning of key enemy military, industrial and administrative facilities and systems, as well as to bring information-psychological pressure to bear on the adversary's military-political leadership, troops and population, something to be achieved primarily through the use of state-of-the-art information technologies and assets.*[96]*"*

The further important subset of goals relevant to cyber-warfare includes any and all operations intent on disrupting the sovereignty or integrity of the targeted nation and its affiliated organs. To wit, the Russian approach to examining what constitutes an act of cyber-warfare is purposefully broad and can be inferred from the nation's overall strategy on utilisation of such operations by the armed forces and intelligence agencies. Russian military doctrine from 2014 is fairly explicit on the perceived threat of cyber-warfare when it enumerated the top external threats to Russia:

> *"Use of information and communication technologies for the military-political purposes to take actions which run counter to international law, being aimed against sovereignty, political independence, territorial integrity of states and posing threat to the international peace, security, global and regional stability*[97]*".*

This is then mirrored by an equally broad internal military threat perception:

> *"Activities aimed at changing by force the constitutional system of the Russian Federation; destabilizing domestic political and social situation in the country; disrupting the functioning of*

[95] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," May 2, 2013, 5.
[96] Roland Heickero, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations" (Swedish Defence Research Agency, March 2010), 17.
[97] Russian Federation, "The Military Doctrine of the Russian Federation."

state administration bodies, important state and military facilities, and information infrastructure of the Russian Federation[98]*".*

Combining the internal and external threat equates to the claim that any attack of significant potency against the state, its various organisations, its citizens or any infrastructure that serves them could constitute an attack worthy of a military response. The irony of this approach is palpable, as Russia has been frequently alleged to conduct such attacks against its neighbours and global peers.

A proper example to the significance of this parameter would be the hack of the US Democratic National Convention (DNC), initially publicised in June 2016[99]. In the incident, a hacker operating under the moniker Guccifer 2.0 released a trove of internal documents emails allegedly exposing the inner workings of the Democratic campaign's seedy underside. While the hacker self-declared himself to be a Romanian hacktivist, extensive analytical commentary by security organisations such as ThreatConnect[100], academics such as Thomas Rid[101] and media outlets such as the New York Times[102] quickly raised the assessment that the attack originated from state-affiliated Russian perpetrators. Rather unusually, attribution to the Russian government itself was publicly acknowledged by the US Department of Homeland Security; "The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails… from US political organizations[103]".

The DNC hack satisfies the target, impact and attacker parameters. However, when observing the assessed goals in compromising a national election race they certainly appear political, yet not military-strategic. While there is extensive potential utility in favourably shaping the US political landscape to better accommodate Russian political grand-strategy, at least the incident itself does not appear to be motivated by a distinct military agenda. Conversely, assessing the 2014 attacks against the Ukrainian voting infrastructure[104] appears markedly different. As military conflict was already in progress in part around the issue of Ukrainian government legitimacy over disputed territories, upsetting the tenets of Ukrainian democracy fuels destabilisation efforts that may then convert to reduced military resolve.

The fifth parameter, *relationships*, can form the strategic demarcation between open hostilities and an otherwise adversarial relationship. Even the gravest of incidents can be overcome if they occur between friendly nations, or otherwise between two parties which have a vested interest in avoiding conflict. Therefore, in order for a network attack to qualify as a warfare-level incident we must

---

[98] Russian Federation.

[99] Tal Kopan, "DNC Hack: What You Need to Know," *CNN*, June 21, 2016, http://www.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/index.html.

[100] ThreatConnect Research, "Shiny Object? Guccifer 2.0 and the DNC Breach," ThreatConnect, June 29, 2016, https://www.threatconnect.com/blog/guccifer-2-0-dnc-breach/.

[101] Thomas Rid, "All Signs Point to Russia Being Behind the DNC Hack," *Motherboard*, July 25, 2016, http://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack.

[102] Nicole Perlroth and Savage, Charlie, "Is D.N.C. Email Hacker a Person or a Russian Front? Experts Aren't Sure," *The New York Times*, July 27, 2016, http://www.nytimes.com/2016/07/28/us/politics/is-dnc-email-hacker-a-person-or-a-russian-front-experts-arent-sure.html.

[103] DHS Press Office, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security."

[104] Margaret Coker and Paul Sonne, "Ukraine: Cyberwar's Hottest Front," *Wall Street Journal*, November 10, 2015, sec. World, http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.

establish the existence of appropriate context, one in which the incident is weaved into the larger political climate and relationship between the involved parties accounted for.

In 2013, online access to multiple US banks was intermittently cut off by a distributed denial of service attack (DDoS)[105]; a form of attack characterised by a large subset of computers overflowing the victim with frivolous data to prevent legitimate access. Denial entails inherently transient attacks, usually incapable of causing permanent damage save financial losses incurred from the temporary lack of access to the victim's services. In this case, the outrage expressed by US officials at the continuous attacks was palpable, with the desire for attribution and retribution mounting.

"There is no doubt within the US government that Iran is behind these attacks,[106]" claimed James Lewis of the Center for Strategic and International Studies, formerly a high-ranking US government official on cyber-security issues. As compelling as the attribution against Iran may have been, it did not result in any significant military action or meaningful retaliation. As expected, the attacks were handled by the judicial system, resulting in a rare indictment of seven Iranian nationals[107]. Notably, this was an action taken against the involved individuals, not the sovereign entity that had seemingly set them on their disruptive course to begin with. As a limited disruptive attack with a political but ultimately non-military goal, it was contained and not pursued further in the international arena.

Examining the first four parameters, at least the first three appear to be distinctly met. It was a successful attack against US critical financial infrastructure, conducted by nation-state affiliated Iranian actors. Arguably, the claim could be made that the impact parameter was similarly insufficient to warrant classification as warfare; but sustained denial of functionality to critical financial institutions may indeed pass this threshold. The fourth parameter does not appear to be easily met, as the goals do not readily translate to a military-strategic agenda. But indeed, even if the banking attacks were military-oriented, it is the existing dynamics of the US-Iran relationship, the deferential character of the Obama administration, and the pre-established behavioural patterns by the US government all cumulatively prevented the fifth and final context parameter from being met.

Political analysis of the United States simply does not corroborate interpretation of the Banking attack as an act of warfare. A powerful regional actor, the United States acted upon its regional agenda to prevent Iranian entrenchment in current and future negotiation of its nuclear capabilities[108], while simultaneously roping its government into a relatively productive role in regional hotspots in Syria, Afghanistan, Iraq, Yemen and Libya[109]. A nexus of Shia influence and a source of funding, military technology and training for many of the US's adversaries, Iran's brinksmanship proved its potency in the way the attack was contained by the United States. It had successfully fashioned a political climate

[105] Nicole Perlroth and Quentin Hardy, "Online Banking Attacks Were Work of Iran, U.S. Officials Say," *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

[106] Perlroth and Hardy.

[107] Duston Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 25, 2016, http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF.

[108] Kenneth Katzman and Paul K. Kerr, "Iran Nuclear Agreement," *Washington, DC: Congressional Research Service*, 2015.

[109] Fawaz A. Gerges, "The Obama Approach to the Middle East: The End of America's Moment?," *International Affairs* 89, no. 2 (2013): 313.

in which conflict was to be avoided unless absolutely necessary. Similarly, the Obama administration has at that point established a prior history of non-reaction, even when faced with adversaries crossing its self-defined red lines for mobilization. Such for example was the case when embattled Syrian president Bashar Assad crossed US President Obama's red line by deploying chemical weapons against rebel forces and the civilian population[110]. The US, in turn, did not implement its own threat, thereby reducing its deterrence and further establishing itself as a noncommittal defender of its own policies and interests.

The context of a sabotaging network attack is thus highly meaningful. Also involving Iran, one of the only confirmed acts of physical damage perpetrated through protracted network operations is Stuxnet, the malware used to retard the Iranian nuclear program by damaging its centrifuges between 2009 and 2011. The case was heavily lauded as the first militarised "cyber-weapon"[111] and a herald of a new era of cyber-warfare[112]. However, deeper observation of the Stuxnet campaign reveals how little it has to do with facilitating war. Perhaps, it even sought to prevent it.

As reported extensively by journalists[113] and information security companies[114], Stuxnet was a clandestine campaign allegedly jointly waged by the US and Israel. While the operation itself was complex, the underlying goals were seemingly straightforward; stunt the accumulation of enriched Uranium by the Iranian government. The goals in turn supported efforts at keeping the possibility of nuclear militarisation distant thereby obviating the need for a military attack against Iranian nuclear facilities. The involved malware was characterised as being highly covert and self-restrictive[115]. Specifically, Stuxnet's developers made exorbitant efforts to conceal its physical disruption from technicians by falsifying maintenance signals[116], thereby opting for gradual, incremental loss rather than a high-profile strike against the Natanz facility. It was an intelligence sabotage operation, managed and conducted by at least one intelligence agency[117], within the scope of a larger political agenda keen on preventing a nuclear Iran without actual warfare taking place.

The Stuxnet attack induces more confusion than clarity. If such a brazen, damaging campaign against a declared enemy nation does not constitute warfare, what does? The incident seemingly ticks most relevant boxes; it was physically damaging, targeted critical national infrastructure, conducted by nation-level actors and served a coercive military-political goal. It is oft cited as the perennial example of cyber-warfare, and yet it was neither predicated nor followed by any other acts of war between the parties involved. A component was thus differentiating this incident from others.

---

[110] James S. Brady, "Remarks by the President to the White House Press Corps," The White House, August 20, 2012, https://www.whitehouse.gov/the-press-office/2012/08/20/remarks-president-white-house-press-corps.

[111] Langner, "Stuxnet - Dissecting a Cyberwarfare Weapon."

[112] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February 2011): 23–40.

[113] David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[114] Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."

[115] It was the alleged failure in self-restriction that caused the malware to infect many unrelated devices, eventually attracting the attention of malware investigators.

[116] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (February 2012): 9.

[117] Sanger, "Obama Ordered Wave of Cyberattacks Against Iran."

The crucial element in which Stuxnet's Operation Olympic Games[118] falls short of warfare is the relationships. The adversarial relationship between Israel, the United States and Iran did not merit the event devolving into a state of armed conflict. Nor was this attack conducted within pre-existing conditions of open hostilities. When separated of such indicators, even a physical network attack may not reach the threshold of warfare if it is not sufficiently damaging or high-profile. Assessing the context of any network attack is therefore critical towards their classification as acts of war.

When is equipment sabotage warfare? The 2007 Israeli operation against the Syrian nuclear Syrian reactor allegedly including a network attack against the Syrian air-defence grid is more thoroughly discussed later in the chapter. It is – if the reported details are correct - the most easily palatable instance of cyber-warfare. When appraising the five elements presented above it becomes apparent that the operation meets all criteria. It was a nation-state actor (perpetrator) attacking a nation-state actor (victim) with significant consequence (impact) for a military-political objective (goal) within the context of a larger kinetic military operation (context) designed to hamstring any attempts by Syria to attain nuclear status. Thus, tactical cyber-operations launched in conjunction with a kinetic attack are perhaps the quintessential embodiment of easily discernible cyber-warfare. But they are not the only such cases.

Borrowing from the Russian doctrinal playbook, mass-impact network attacks on civilian infrastructure may be a notable subset of warfare-level operations. If a nation-affiliated actor strikes at a nation-affiliated adversary with an attack designed to severely impact civilian life, the conduct of warfare my appropriately apply. It must, however, meet all parameters to properly qualify. As a result, such an attack must either be a prelude or in tandem with other acts of violent aggression and be sufficiently impactful as to cause severe disruption or harm. Finally, there must be an underlying military political goal rather than a criminal one, a goal reflecting the national agenda espoused by the attackers.

Re-examining the alleged Russian network attack against the Ukrainian power station with the aid of the five accumulative parameters shows it too does not reach the threshold of warfare, though it comes very close. On the affirmative side, the attack was supposedly conducted by a nation-state participant in the form of Russian security services and targeted Ukrainian critical infrastructure[119]. As there are intermittent active hostilities between Russia and the Ukraine over Crimea and its adjacent territories[120], the context parameter is also fulfilled. However, the attack itself was of limited impact and did not appear to contribute to the larger regional military goals. Instead, the two unmet parameters – impact and goals - indicate the attack was intended as a political signalling in the form of digital sabotage, which would likely not (and did not) result in escalated hostilities. Were the power grid attack geared towards creating greater damage in order to directly coerce the Ukrainian

[118] Sanger.

[119] United States Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT," ICS-CERT, February 25, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[120] Russian military activity in Eastern Ukraine has not been publicly acknowledged as active warfare by the Russian government. Numerous indications of Russian troops have been rigorously denied and countered by information operations, discussed at a later chapter.

government into altering its strategy on its eastern borders, it would successfully meet all criteria of cyber-warfare. Operational success was not even necessary, merely the visible intention to create a significant effect within a military context.

To conclude, offensive network operations embody the continued evolution of warfare as a result of the adoption of networked hardware into every aspect of modern living. While demonstrable acts of cyber-warfare are rare, the discussions conducted by various nations on the role of cyber-warfare within their national doctrines and the threats emanating from cyberspace is highly edifying when attempting to frame cyber capabilities as tools of war. Some of the examples used within this chapter are more palatable than others, but by utilising the five provided parameters, assessing network intrusion incidents becomes a more direct endeavour. Were it applied to most of the instances widely panned as warfare in modern journalism and novels, it would show that most incidents are wholly outside the boundaries of warfare. The global state of cyber-warfare is actually quite calm.

The spectrum of cyber-warfare includes attacks which are either directly supporting kinetic campaigns, or are otherwise generating an impactful influence upon the adversary within a larger military-political context. When viewed thusly, only a very specific – but still significant – subset of operations is included. Upon reaching this standardization, inspection of the advantages and disadvantages of cyber-warfare and their larger role within conflict becomes a more feasible endeavour to undertake. War remains a violent struggle between groups vying to upset the existing power dynamics, and offensive network capabilities do not as radically alter this underlying truth.

CYBERWAR & CYBERWARFARE

The inescapably political nature of war presents the first challenge to assessing cyberwar as an term of art. As Kenneth Waltz once posited, "War begins in the minds and emotions of men, as all acts do"[121]. Warfare has changed, but its fundamental tenets have not. While warfare may rely on increasingly complex tools, it remains at heart a contest between people. Computers, devices or networks cannot declare and wage war against one another, at least not yet. Therefore cyberwar – if at all a valuable concept - is simply war as waged by actors through the use of computers and networks.

It is curious to note how prevalent the use of cyberwar is, as if wars can be waged and won through network attacks alone. War does not routinely restrict itself to a single domain be it land, sea, air, or indeed cyberspace. Basil Liddell Hart's suggestions in 1952 that "Airpower might attain a direct end by indirect means[122]" did not assert itself as a viable ethos for winning wars. As NATO realised in Kosovo, as the United States experienced in Iraq, and as Israel internalised in Lebanon[123], avoiding entire domains in favour of safer, indirect forms of warfare merely delays and intensifies future cross-

[121] Waltz, Kenneth, *Man, the State, and War: A Theoretical Analysis* (Columbia University Press, 2013), 9.
[122] B.H. Liddell Hart, "The Objective in War," *Naval War College Review* 5, no. 4 (December 1952): 13.
[123] In the Second Lebanon War of 2006, Israel favoured its air force in the early days of conflict, with limited strategic success.

domain warfare. In this respect, Waltz's remarks proved prescient once more; "In reality, everything is related to everything else, and one domain cannot be separated from the others[124]".

Cyberwar is ubiquitous because it is conflated with cyber-warfare. Cyberwar too often encompasses acts of aggression that do not equate to war, threading those together in a narrative of conflict limited to digital means. Much like previously vaunted theories of complete battlefield dominance through overwhelming airpower, offensive network capabilities are unable to singularly achieve political goals. In the opening chapter to their oft-referred book *Cyberwar*, Richard Clarke and Robert Knake artistically depict the suspected use of offensive network capabilities in 2007. Israeli air force (IAF) warplanes supposedly bypassed the thick Syrian air defences to clandestinely strike at the Kaibar nuclear reactor in Deir-Azzor[125]. While this attack is arguably one of the most easily classifiable publicly known instances of cyber-warfare[126], it falls short as a depiction of cyberwar. Irrespective of the role of offensive network capabilities in the strike, it was guided bombs and missiles that reduced the facility to ruin. The Israeli incident is a textbook depiction of a combined arms package, in which an alleged network attack enabled an immediate kinetic strike for lasting effect. The political objective underpinning the conflict, which was to curtail non-conventional abilities that would upset the strategic balance in the Middle-East, was supposedly achieved by jointly operating cyber and air power.

Viewed independently, the Israeli incident is a shining example of cyber-warfare as an integrative capability rather than a standalone domain of warfare. It does not validate the existence of cyberwar; there was no reciprocal conflict waged through networks. Where war is an exercise of aggression to attain political goals, offensive network capabilities are poorly positioned to single-handedly ensure success. Analogising this to other domains of warfare, the fallacy of this perceived reality becomes readily apparent; modern wars to not neatly constrain themselves to a single domain or set of capabilities. To analogise, renowned naval strategist Alfred Thayer Mahan posited heavily upon the momentousness of the naval arena in power struggles between nations[127]. He did not, however, decree that naval engagements exist in a vacuum, devoid of additional domains of warfare.

Analysis of modern warfare can benefit from setting aside cyberwar as a concept. Instead it is more useful to observe cyber-warfare as a set of integrative offensive network capabilities used to engage an adversary in a period of armed conflict. By emphasizing cyber-warfare as part of a broader tapestry of armed conflict, we discount the notion that network intrusions are immediately indicative of an overall, war-level conflict between two or more parties. Focusing on operations rather than war then leads to a range of critical questions about the utility and role of networked capabilities. Can network attacks trigger war? What forms of network attacks fall within the remit of warfare and which are

---

[124] Kenneth N. Waltz, "The Origins of War in Neorealist Theory," *Journal of Interdisciplinary History* 18, no. 4 (1988): 615.

[125] Richard A. Clarke and Robert K. Knake, *Cyber War: The next Threat to National Security and What to Do about It*, 1st ed (New York: Ecco, 2010), 9.

[126] The final part of the chapter revisits Operation Orchard in order to examine how it is indeed one of the only instances that fully align with an acceptably standard definition of cyber-warfare.

[127] Alfred Thayer Mahan, *The Influence of Sea Power upon History, 1660-1783* (Read Books Ltd, 2013).

merely acts of espionage or sabotage? As the next chapter details, MONOs are in fact more similar to electronic warfare than they are to the other distinct battlefield domains – air, sea, land or even space.

"It is not correct to call every bad thing that happens on the internet 'war'…", correctly exclaimed James Lewis in 2010 in his paper titled "Thresholds for Cyberwar"[128]. Around that time, many network intrusions and even rudimentary scanning attempts were problematically and incorrectly labelled as attacks[129]. Tallies were inflated to enormous, unfathomable numbers to present an alarming image of constant digital warfare occurring between global political adversaries. Thankfully, coverage of digital warfare has since vastly improved, though a problematic narrative persists somewhat.

A well-established approach is to classify network warfare as a subset of information warfare conducted through computers and networks[130][131]. As a notable example, the Russian military has no independent conceptualisation of "cyber" except when remarking on Western doctrine[132]. Instead, warfare conducted via the internet or against enemy networks is folded into the struggle for information dominance, one pursued aggressively by Russia[133]. By adopting this approach, networked attacks operate within similar parameters to electronic warfare, information warfare and psychological operations.

Lumping electronic warfare with cyber-warfare is attractive. Much like electronic warfare, offensive network operations seek to disrupt, alter, corrupt or otherwise influence the operation of the targeted system. While classic electronic warfare most often seeks to achieve this by emitted radio frequency (RF) transmissions, cyber-warfare attempts to achieve the same by interfacing directly with the targeted system's hardware and software. The attack vector may differ; the underlying logic and desired effect often remain the same.

The Russian government has visibly adopted this approach in its political and military manoeuvers, yet it is not singularly Russo-centric in nature. In 1999, John Arquilla - a notably early scholar of cyber-warfare – revisited his previous statements and claimed that "information warfare is a concept that ranges from the use of cyberspace to attack communication nodes and infrastructures to the use of information media in the service of psychological influence techniques[134]". Arquilla's RAND colleague Martin Libicki expressed a similar sentiment as early as 1995[135]. As the United States gradually became more transparent in its acknowledgement of offensive network capabilities, the Department of Defense's 2003 Information Operations Roadmap initially outlined the perspective in

---

[128] James A. Lewis, "Thresholds for Cyberwar" (Center for Strategic and International Studies, 2010), 1.

[129] See for example; Sam Jones, "Ministry of Defence Fends Off 'Thousands' of Daily Cyber Attacks," *Financial Times*, June 25, 2015, https://www.ft.com/content/2f6de47e-1a9a-11e5-8201-cbdb03d71480.

[130] Raymond C. Parks and Duggan, David P., "Principles of Cyber-Warfare," in *Proceedings from the Second Annual IEEE SMC Information Assurance Workshop* (New York: West Point, 2001), 122.

[131] Rattray, *Strategic Warfare in Cyberspace*.

[132] Ulrik Franke, "War by Non-Military Means," 2015, 34, http://www.foi.se/ReportFiles/foir_4065.pdf.

[133] Keir Giles, "'Information Troops'-A Russian Cyber Command?," in *3rd International Conference on Cyber Conflict*, 2011, 46.

[134] John Arquilla, "Ethics and Information Warfare," in *Strategic Appraisal: The Changing Role of Information in Warfare*, ed. Zalmay Khalilzad, John P. White, and Andrew Marshall (Santa Monica, CA: RAND, 1999), 380.

[135] Martin C. Libicki, *What Is Information Warfare?*, 3rd edition (Washington DC: National Defense University, 1995).

which electronic warfare and computer network operations are viewed as equally significant pillars of information operations[136]. In an unusually motivational-like phrasing the document awkwardly declared; “We Must Fight the Net.”

Russia is unusual as its approach to information warfare audaciously blends the civilian with the military, influence with coercion, and the digital effect with the kinetic. It does not matter whether a general seeks to influence global perception of Russian forces or achieve command and control dominance in a battlefield – it all falls under the purview of offensive information operations. Controlling the flow and shape of information is thus a key tenet of modern Russian doctrine. An approach clustering different facets of manipulating the flow of information is understandably useful. The digital building blocks that make up civilian communication are often highly similar when broken down. Networks of different types, sizes and purposes often use the same protocols and thus can be targeted in similar ways. Where manipulating computer networks may yield military results one day, it may similarly disrupt the flow of terrorist propaganda the next. But herein the similarities end.

There are important limitations to the Russian perspective. A monolithic approach to information operations may risk muddling the important distinctions between its different sub-categories. When providing the military and supporting security organisations carte blanche to conduct full spectrum information warfare across all targets and agendas, the results may bleed into one another with reduced effectiveness. The degree of finesse required in order to successfully influence mass global media is incomparable to disconnecting aircraft from their regional command. Where the former relies on subterfuge, nuance and an intimate socio-cultural familiarisation with the target, the latter requires technical acumen and an operational intelligence cycle to breach hardened networks and identify vulnerabilities[137].

A secondary risk by blurring the boundaries between information warfare and militarized cyber-warfare is undue escalation. Simply put, if information operations are within the discussion of war, even low-yield, minimally affective operations may be treated as *jus ad bellum*. We must then consider whether an American digital influence campaign in occupied Crimea desirably constitutes an act of war against Russia. Information operations are pervasive in peacetime as a means of manipulating the political landscape to generate favourable conditions. Affixing such operations to the spectrum of war greatly increases the risk of friction between otherwise low-contact adversarial relationships.

An alternate way to observe the development of cyber-warfare is as a counter-innovation phenomenon. In this view, rather than the pristine outlook of offensive network capabilities as independent means of securing battlefield goals, these toolsets become means to offset the capability of the adversary to achieve said goals. It is an evolutionary concept, borne as a response to the rise of the interconnected battlefield. Where digitisation and networks have once enabled the precise,

[136] U.S. Department of Defense, “Information Operations Roadmap” (U.S. Department of Defense, October 30, 2003), 9.

[137] The unique characteristics of offensive network operations are covered in a subsequent chapter, alongside their associated risks and opportunities.

coordinated operations of the 21st century, we now see the techniques that materialise to mitigate them.

The People's Republic of China (PRC) is a staunch advocate of this doctrine, and understandably so. During the First Gulf War of 1991, Chinese military leadership were suddenly in full view of a revolutionary theatre-level campaign against the Iraqi military[138]. The US-led military coalition assembled to expel Saddam Hussein's Republican Guard from Kuwait was so successful as to result in near-surgical evisceration of Iraq's conventional forces, previously considered to be well-trained, well-equipped and capable. Precise joint operations were made possible by the interleaving of intelligence, surveillance and reconnaissance assets (ISR) with guided ordnance. Data from ISR assets was fed into command and control centres of gravity which allowed effective operational decision making on an unprecedented scale.

This new approach was later coalesced into the US Network-Centric Warfare doctrine. It was defined as focusing "…on the combat power that can be generated from the effective linking or networking of the warfighting enterprise[139]". Integration of digital networks into the full range of wartime decision would significantly enhance the quality, quantity and response rate of actions taken. Sensors from assets deployed both within and without the battlefield were to provide critical mission support and assist in dispelling the fog of war. To nations such as the PRC, which were – at the time – gradually increasing the indigenous investment into modernisation efforts of their armed forces[140], observing joint warfare in its full capacity was alarming.

Lessons learned from observing integrated coalition forces in the Gulf War were eventually co-opted into PRC operational doctrine. The People's Liberation Army was directed towards focusing on integrated joint warfare as a key means of defeating asymmetrically preferable adversaries. As explained in the key account of Chinese People's Liberation Army (PLA) strategy, "The Science of Military Strategy", achieving this reality was made (and remains) uniquely possible by increasingly adopting information sharing on an operational level: "[s]upported by information technology… various combat factors are woven into a unity[141]".

From network-centric warfare grew the PRC's brand of network warfare as a form of military counter-culture. When the PRC internalised that their conventional forces were heavily outmatched, it resulted in concerted effort to rebalance this asymmetry by turning the unique characteristics of the US command and control structure into a vulnerability[142]. If all battlefield operations were now reliant

---

[138] Anthony H Cordesman et al., *Chinese Military Modernization and Force Development: A Western Perspective* (Washington, D.C.: Center for Strategic and International Studies, 2013), 54.

[139] David S. Alberts, John Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series (Washington, DC: National Defense University Press, 1999), 88.

[140] Cordesman et al., *Chinese Military Modernization and Force Development*, 1–2.

[141] Cordesman et al., 57.

[142] Larry M. Wortzel, "PLA Command, Control and Targeting Architectures: Theory, Doctrine, and Warfighting Applications," *Right-Sizing the People's Liberation Army: Exploring the Contours of China's Military* 197 (2007): 191, http://kms1.isn.ethz.ch/serviceengine/Files/ISN/48444/ichaptersection_singledocument/8c5607a1-4ad7-46d3-8490-22fc612f3002/en/Chapter%205.pdf.

upon timely, consistent and numerous data inputs from multiple sensors, interrupting this flow could potentially wreak havoc upon the adversary.

China's new approach to counteracting the advantage of C4ISR systems was pithily labelled "local wars under the conditions of informationisation[143]". Although cyberspace was viewed holistically in the PRC's national strategy as a "… new pillar of economic and social development[144]", it was also immediately christened an altogether new domain of national security[145]. Within this doctrine, degrading or disabling the adversary's information hubs became paramount towards attaining initial operational dominance, thereby facilitating subsequent victories on the battlefield.

The PLA's views on digital warfare - which hold numerous similarities to their US counterparts[146] – characterize offensive network capabilities as a combined arms package to be employed alongside kinetic hard kill operations[147]. In this sense, attacks targeting computer software are a crucial asset for the modern warfighter, as they deny adversary capabilities, reduce threat and enable kinetic operations. This perspective reflects the evolution of PLA doctrine to react to the primary processes undertaken by its adversaries. While the true potency of the PLA's militarized offensive capabilities remains uncorroborated, the focal shift reflected in official writing and organizational changes is telling. However publicly visible the adoption of offensive network operations seems to be, it is not the PLA that has been the purest embodiment of the integrative approach, but rather Israel.

As previously mentioned, in late 2007, numerous international media outlets reported a surprise airstrike against a previously publicly unknown Syrian nuclear facility in Deir Azzor[148]. The strike was widely and immediately attributed to the Israeli Air Force, known for its adoption of a proactive operational doctrine bent on preventing regional powers from attaining the capability to produce nuclear weapons. The results were staggeringly successful; complete destruction of the facility, wide international condemnation after a follow-up UN-sponsored probe confirmed the presence of nuclear materials[149] and perhaps most importantly – no retaliation from the incensed Syrian regime. It was a clear tactical, operational and strategic success for the aggressors.

Breaching the Syrian air defences to accomplish a surgical strike with no friendly casualties, loss of materiel, and minimal collateral damage is especially noteworthy when matched with the perceived high quality of Syrian air defences[150]. Known as the most tightly-interwoven modernised air defence network in the region, it surprised many to learn that it never fired a shot at the transgressing warplanes. The question of how this came to pass lingered in the wake of the irradiated ruins of the facility. Five years later, in September 2012, the New Yorker published a lengthy investigative piece on

---

[143] The State Council Information Office, China's Military Strategy.
[144] The State Council Information Office.
[145] The State Council Information Office.
[146] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," May 2, 2013, 6.
[147] Cordesman et al., *Chinese Military Modernization and Force Development*, 58.
[148] David E. Sanger and Mark Mazzetti, "Analysts Find Israel Struck a Syrian Nuclear Project," *The New York Times*, October 14, 2007, http://www.nytimes.com/2007/10/14/washington/14weapons.html?_r=0.
[149] Peter Crail, "IAEA Sends Syria Nuclear Case to UN," Arms Control Association, July 7, 2011, https://www.armscontrol.org/act/2011_%2007-08/%20IAEA_Sends_Syria_Nuclear_Case_to_UN.
[150] O'Conner, "Access Denial - Syria's Air Defence Network," 1.

the attack in which it was claimed that the Israelis were "…using standard electronic scrambling tools…" to effectively blind Syria's anti-air radars[151].

Conventional jamming against such a sprawling network is risky. Syrian forces operate a wide range of anti-air assets, ranging from older SA-2 and SA-6 batteries that are susceptible to older forms of jamming, to more modern SA-17 Buk and SA-22 Pantsyr-M1 batteries purportedly sporting significant jamming resistance[152]. A larger, "hotter" strike could have included aircraft carrying high-speed anti-radiation missiles (HARMs) designed to physically eliminate radar-emitting anti-air threats, or the use of Israeli home-grown standoff cruise missiles such as the Popeye or Delilah. High-profile kinetic attacks would have undoubtedly raised the calculus of brinksmanship, risking cornering Syrian President Bashar Assad to an otherwise undesirable escalatory reaction. Israeli decision-makers acknowledged the significance of maintaining low attack profile, opting for the limited "Thin Shkedi" operational package (so named after then air force commander Eliezer Shkedi) rather than the wider, more comprehensive "Fat Shkedi[153]".

A network attack against the Syrian air defense grid has been widely suggested as a crucial enabler of the overwhelming Israeli success. While this is as of yet unconfirmed by official sources, the arguments for the use of offensive network capabilities are sound. A non-lethal network attack is advantageous as it results in a low-profile, deniable disruption to adversary systems, thus carving out a window of operations for incoming aircraft while avoiding meaningful collateral damage. While Israeli capabilities in this field are largely unproven, US reporting has previously covered the suspected existence of an airborne anti-platform cyber-warfare platform dubbed Suter, allegedly developed by British security company BAE Systems[154]. If a network attack was indeed employed, it is one of the only publicly discussed combined-arms military use of offensive network capabilities. The attack embodies the significance of software-based strike vectors as key enablers and supporters of physical follow up attacks. A joint-warfare doctrine which incorporates network attack elements can in turn expose critical vulnerabilities in an otherwise potent adversary, lending key advantages to an enterprising attacker.

The United States armed forces have over the last 20 years increasingly identified the importance of information systems to modern warfare. In 1998, Cebrowski and Garstka of the US Navy notably penned a piece in which they claimed that the U.S was "…in the midst of a revolution in military affairs (RMA)[155]". They were referring to the importance of the "fundamental shift from… platform-centric warfare to… network-centric warfare[156]". By that time, the revolutionary perspective on cyber-warfare has been long time in the making within the US Department of Defence. The speed and

---

[151] David Makovsky, "The Silent Strike," *The New Yorker*, September 17, 2012, http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.

[152] "Syria: Foreign Intervention Still Debated, but Distant," *Strategic Comments* 18, no. 6 (August 2012): 1–5.

[153] Makovsky, "The Silent Strike."

[154] Clay Wilson, "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues" (DTIC Document, 2007), 7, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA466599; Clarke and Knake, *Cyber War*, 10.

[155] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," in *US Naval Institute Proceedings*, vol. 124, 1998, 25.

[156] Cebrowski and Garstka, 25.

quality of wartime decision making could be markedly improved by harmonizing different platforms and sensors to seamlessly work together. The contributory power of the network far exceeded the sum of its nodes.

The rise of network-centric warfare and cyber-warfare are tightly correlated. As US forces increased their reliance on sensory networks and complex command and control grids, they realised the potential to weaponise the very same phenomenon against potential adversaries. The command and control network became the digital embodiment of the Clausewitzian centre of gravity; "[it] is always found where the mass is concentrated most densely. It presents the most effective target for a blow[157]". Rather than classically delivering a crippling blow to an enemy's force concentration the aggressor could instead target the nerve hub of its operations, thereby fulfilling Clausewitz's intended goal of unsettling the enemy's balance[158]. If battlefield awareness and the capacity to operate swiftly, accurately and jointly now predicated on the unrestricted flow of data, a blow against the nerve centre that oversees this process could be pivotal for strategically influencing the entire war effort.

Further building upon its importance, the United States gradually adopted an approach framing digital attacks as an independent domain of warfare. The conversation in the US military and government over the role of cyber-warfare has been an evolutionary one; from a minimal acknowledgement of information operations to a fully-budgeted Cyber Command, standalone doctrine[159] and dedicated exercises. As defined in 2005 by then Air Force Secretary Michael W. Wynne, the new role of the air force would henceforth be to "…to fly, and fight in Air, Space and Cyberspace[160]". The US perspective codified cyber-warfare as a distinct field, with its own set of rules and considerations.

The distinct domain approach is gaining traction in the West. After attributing several Russian-attributed network attacks against Estonia and Georgia in 2007 and 2008 respectively, an alarmed NATO scrambled to come to grips with the vulnerability of its member nations' networks and its own incapacity to conduct effective wartime operations in cyberspace. Most immediately, NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) solicited a group of experts led by Michael Schmitt to identify the circumstances under which network attacks constitute *jus ad bellum*, thereby qualifying above the threshold of warfare[161]. In 2014, NATO expanded its defensive ethos to incorporate a network attack as a legitimising catalyst for invoking Article 5, which covers NATO protocol in the case of an attack against a member state[162]. Eventually in July 2016, NATO

[157] Carl Von Clausewitz, *On War*, 3rd ed., vol. 1 (London: N. Trubner & Co, 1873), 485–87.
[158] James Schneider and Lawrence L. Izzo, "Clausewitz's Elusive Center of Gravity," *Parameters*, September 1987, 48.
[159] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," May 2, 2013.
[160] Mitch Gettle, "Air Force Releases New Mission Statement," United States Air Force, December 8, 2005, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/132526/air-force-releases-new-mission-statement.aspx.
[161] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).
[162] Steve Ranger, "NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict," *ZDNet*, June 30, 2014, http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.

conventional wisdom coalesced around a declaration mimicking their US member state doctrine; cyber was announced to be a distinct domain of warfare alongside air, sea and land[163].

Different nations adopt disparate approaches to cyber-warfare. Some choices more thoroughly adhere to the distinctions that make the intangible software space unique; the United States visibly fences operating within and against networks militarily, more naturally adhering to the five-step model. Conversely, Russia recognizes the added value of cyberspace, but does not necessarily expose the seams between those who fight within the domain and those who fight without. Networks are thus a virtual medium through which existing doctrine and operating procedures are channelled and reflected. The more integrative approach to MONOs means that they often purposefully fly below the model threshold, in a bid to avoid countermeasures. China views network operations as an equaliser, an opportunity to shatter existing symmetries and turn the advantages embodied in modern networked warfare into vulnerabilities. Lastly, countries such as Israel retain ambiguity over the actual doctrine surrounding cyber-warfare, but appear to be employing it nonetheless as a combined arms package in support of kinetic operations.

Approaches to digital warfare may vary, yet they crucially intersect where operations meet wartime necessity. It is the need forcefully erode the will of the enemy (conjuring Clausewitz once more)[164], or alternatively seek to complement ongoing war efforts. A scope for cyber-warfare must encompass this reality, as has been shown throughout this chapter. While the major wielders of offensive network capabilities vary in their perception of their utility and the terminology used to describe them, they intersect on doctrine and deployment more than it initially seemed.

To conclude, cyber-warfare is commonly viewed as designed to contribute to joint efforts to affect information for military-strategic goals. The above analysis is complemented by several high-level observations. The first is that offensive network capabilities cannot single-handedly achieve strategic objectives; such capabilities are best used when complemented by others. For some such as the United States it may entail incorporation into kinetic strikes, while others – namely Russia – place more significant weight on large-scale information operations that include psychological warfare. As a corollary, offensive network capabilities are consensually viewed as integrated into the spectrum of information operations. Finally, MONOs are a natural evolution of warfare and doctrine, as they gradually formed out of a modern-day dichotomy; the need to offset the strategic advantages of a highly-networked force, while simultaneously capitalising on the strategic vulnerabilities of the highly-networked nation which it defends.

[163] Eimi Harris, "NATO Adds Cyber to Operational Domain," NATO Association of Canada, July 4, 2016, http://natoassociation.ca/nato-adds-cyber-to-operational-domain/.

[164] Schneider and Izzo, "Clausewitz's Elusive Center of Gravity," 56.

2. CHARTING INTANGIBLE WARFARE

OVERVIEW

A century has passed since warfighting first engaged with the electromagnetic spectrum. While the study of war often focuses on the kinetic, it is the imperceptible mediums that have contributed some of the greatest leaps to the modern battlefield. From the advent of radar in the years leading up to the Second World War to vying for digital information superiority today, war waged through invisible means has enmeshed itself in every nation's doctrine. Cyber is the first aspect of intangible warfare to be widely recognized as sufficiently distinct as to merit its own domain of war. But how truly different is it from its predecessors? How unique are its characteristics, associated challenges and operational parameters?

This chapter argues that *numerous attributes uniquely attributed to cyber-warfare have been previously associated with warfighting in the electromagnetic spectrum*. As a corollary, examining similar concepts such as electronic warfare, electromagnetic warfare, command and control warfare, information operations and cyber operations, will be shown to be sufficiently related in their characteristics as to be bundled together under the term *intangible warfare*. The chapter is therefore not intended to be a literature review, but rather a deconstruction of MONOs that demonstrates their unbreakable familial relation to electronic warfare. Efforts to separate them entirely are therefore often artificial, as are some observations on cyber as the first man-made domain of war.

Offensive cyber capabilities are therefore an evolutionary concept representing seven decades of cumulative experience and development in other forms of intangible warfare. The fundamental necessity to be intimately familiar with the particular equipment being targeted dates to radar jamming efforts in the Second World War, as is the notion that employing such capabilities may lead to their loss due to detection. The Cold War saw strategy evolve from deceiving operators to directly impacting the functionality of devices and equipment. Perhaps most importantly, the idea that situational awareness on all levels – tactical, operational and strategic – can be critically manipulated by non-kinetic capabilities has coalesced over the span of the last five decades.

Whereas bullets, shells and missiles function as intended against a wide range of possible targets, intangible warfare is unique in such that it may require the development of tools designed to defeat a particular enemy's specific technology. From the Second World War era of British attempts to jam German flight guidance radar to intricate network operations against military platforms done today, both share the undeniably crucial need for intelligence and familiarization with the adversary. Aspects of intangible warfare both historic and modern represent the desire to increasingly weaponize the adversary against itself and erode the fundamental trust a battlefield commander places in their technological toolset.

In some respects, cyber-warfare is not a distinct domain of warfare. Much like electronic warfare, battlefield cyber-capabilities may separately affect targets but are almost always wielded by operators in the classic domains of war – land, sea and air. Understanding this integrative notion analytically then provides researchers and practitioners the ability to implement lessons learned from previous iterations of intangible warfare – in doctrine, strategy, operations and incorporation of new technologies and capabilities.

Already in 2001, then US Air Force officer Gregory Rattray railed against the supposed novelty of so-called cyber warfare. Particularly, Rattray rejected "…the assumption that strategic information warfare should be treated as a completely new phenomenon because of the 'virtual' or nonphysical nature of operating in the cyberspace environment[165]". While this chapter shares that premise at its core, Rattray then proceeded to assess offensive network capabilities against as an evolution of strategic air warfare[166]. Indeed, the analogy to the early days of air warfare is apt when discussing how network operations are described but it does little to explain how they differ from traditional warfare. So instead, this chapter will establish the claim that it is an evolution of other forms of intangible warfare.

The chapter unfolds by reviewing a century of literature and warfighting, dating to the inception of combat electromagnetic means. The analysis is ordered chronologically, examining in sequence the two World Wars, the Cold War period, the dawn of network-centric warfare in the 1990s, and the subsequent global rise of information operations. With each such iteration, intangible warfare matured and accrued more of its modern characteristics. As the analysis will show; cyber-warfare today did not materialize suddenly with the onset of the internet. Offensive network operations are reflective of a century of doctrinal and strategic bricklaying.

While the rapid cycle of innovation and counter-innovation will gradually be demonstrated to be a core commonality of all aspects of intangible warfare, it did not originate with it. The requirement for technological advancement in order to remediate adversary advantages has always played some role on the battlefield. Personal armour was introduced to reduce the kinetic impact of blows and arrows but was later rendered less effective with the advent of gunpowder. Stone fortifications were countered by increasingly sophisticated siege equipment from trebuchets to catapults, mechanisms designed to return the offense-defence balance to an acceptable equilibrium. For centuries, development cycles were glacially paced[167]; the scientific method and overall prevalence of battlefield technologies had limited significance to warfare. This is not a novel observation, as Clausewitz once remarked in his writings: "Fighting has determined everything appertaining to arms and equipment, and these in turn modify the mode of fighting; there is, therefore, a reciprocity of action between the two[168]". Yet at the time, strategy, manpower and logistics were vastly more important.

---

[165] Rattray, *Strategic Warfare in Cyberspace*, 17.
[166] Rattray, 66.
[167] Rattray, 165.
[168] Clausewitz, *On War*, 1:73.

It was chiefly in the First World War when technology became a significant strategic element. While some of the war's belligerents - such as the British military - adopted key elements of technology-laden warfare even prior to the war[169], it was only tested at scale when open combat erupted. Uniquely at the time, the incorporation of technological advancement heavily influenced doctrine. The oft-recited perception of the First World War as one of trenches and attrition was in part due to the then-conventional wisdom that the introduction of machine guns meant open warfare doctrine was rendered obsolete; technology has now lent to its wielders an unstoppable killing power that could not be directly countered. Commanders and strategists suddenly had to become innovators[170]. Although some Allied commanders such as the American Expeditionary Forces commander in chief John Pershing held to their refusal to alter doctrine to compensate for new threats[171], the field of war inexorably changed.

So dawned the first cycle of modern military counter-innovation. As military historian Shimshoni aptly observed of the First World War's evolutionary doctrine; "…technology (doctrine) and applications (war plans) interact in a cyclical manner, in the quest for integration[172]". The necessity to counter asymmetry-inducing technologies meant that both existing tools had to be wielded better, and new tools developed. The lagging in adjusting to new battlefield realities is in part the reason for the war's drawn out campaigns, with battles ending in unfathomable death counts on all sides[173]. Doctrine gradually adjusted with the first large-scale use of joint operations combining infantry, creeping barrages of artillery and to a degree – tanks. These new inventions – ushered by British forces in 1916 late into the war – were seen as a stalemate-shattering technological advancement capable of once again upsetting the offence-defence balance[174].

First Cycle – The Second World War

In 1939, British intelligence officers in Oslo received an anonymous tip. They were instructed to adjust the daily BBC World Service German-language news broadcast slightly to signal the presumably German turncoat to provide the information he offered. They did, and after calling out "Hello, hier ist London", they subsequently received a staggeringly comprehensive report on cutting edge German technological developments. These included details of large military radars being developed and deployed, of large-scale rockets and even unmanned aerial vehicles[175]. Successfully co-opting the use of radar had seemingly allowed the Germans to circumvent one of the greatest challenges that plagued both the German Luftwaffe and its allied counterparts –conducting precision night-time aerial bombing runs, when anti-aircraft guns were blind[176].

---

[169] Hew Strachan, "The Battle of the Somme and British Strategy," *Journal of Strategic Studies* 21, no. 1 (March 1998): 81.
[170] Jonathan Shimshoni, "Technology, Military Advantage, and World War I: A Case for Military Entrepreneurship," *International Security* 15, no. 3 (1990): 190.
[171] James W. Rainey, "Ambivalent Warfare: Tactical Doctrine of the AEF in World War I," *Parameters* 13, no. 3 (1983): 34–46.
[172] Shimshoni, "Technology, Military Advantage, and World War I," 199.
[173] Shimshoni, 211.
[174] Shimshoni, 207.
[175] Reginald V. Jones, "Scientific Intelligence," *Journal of the Royal United Service Institution* 92 (1956): 55–56.
[176] Jones, 61.

As Reginald Larson - one of the fathers of modern Western intelligence – recounts, British agents soon confirmed the existence of a German blind-bombing radar-based system known as *Knickebein* ("Crooked Leg"), codenamed "Headache" by British forces[177]. The radar was an ingenious invention in which two radio beams were transmitted in slightly different patterns from two locations in occupied France's coast, the beams calculated to intersect roughly over targets in the United Kingdom. Luftwaffe bombers would then fly along one beam until their receivers indicated they reached the transmission intersection and released their payloads. British intelligence launched an exploratory sortie in June 1940 intent on intercepting these German radar transmissions[178]. Their efforts bore fruit and resulted in the development of a crude jammer with the humorously appropriate codename; Aspirin[179].

The British countermeasure did not spell the end of what later came to be colloquially called "The Battle of the Beams". Aside for waging actual warfare, both parties were now thoroughly engaged for the first time in history in a brief but fast-paced battle of technological wit. The Germans had not yet given up on electronically transmitted guidance systems, deploying the successful X-Gerät (X-Device)[180] radar in late 1940 with improved jamming resistance[181]. This in turn was countered again by the British, which led to the far less successful Y-Gerät – or Wotan II - in 1941. By that time and aided by Enigma-decoded information, British intelligence had anticipated the deployment of Y-Gerät, rendering it entirely ineffectual[182]. Soon after, the Germans were forced to recall their efforts as attention was redirected towards the build-up on the Eastern front, where an invasion into Soviet territory was imminent.

The contest over radar dominance in the Second World War was the first large-scale instance of what shall henceforth be called *intangible warfare*; the adoption of intangible means of warfighting such as electromagnetic transmissions and later attacks against digital networks. Much like the data-based attacks often discussed today within the remit of cyber-warfare, even the earliest forms of intangible warfare included much of the same characteristics, ranging from often imperceptible effects to the caution in employing measures as to avoid exposing their existence to the adversary. The Second World War - in this regard – would be the dawn of modern intangible warfare.

In the years leading up to the Second World War it became increasingly clear that technology now played a pivotal role in developing modern strategy. The Great War saw an entire generation decimated due to previously unseen firepower. In the war's aftermath, it soon grew apparent that new capabilities and techniques were needed to increase combatant survivability and once again produce a favourable flow of combat. Thus, the interfering years between the two World Wars saw an explosion of new technology. Major developments included the formalization of air as a strategically pivotal

---

[177] Robert W. Burton et al., *The Strategy of Electronic Warfare* (U.S. Air Force Academy, 1979), 4.
[178] Jones, "Scientific Intelligence," 61.
[179] Alfred Price, *Instruments of Darkness* (Barnsley, UK: Frontline Books, 2017), 82–83.
[180] Also called Wotan in German encoded communications
[181] Robert Cockburn, "The Radio War," *IEE Proceedings A-Physical Science, Measurement and Instrumentation, Management and Education-Reviews* 132, no. 6 (1985): 426, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4647746.
[182] Jones, "Scientific Intelligence," 63–64; Cockburn, "The Radio War," 428.

domain of combat, wide adoptions of armour corps, initial forms of rocketry and indeed, the dawn of computing and electromagnetic transmissions for communications, navigation, and remote object detection. The groundwork was thus laid to graduate beyond the initial cycle of counter-innovation to one to including intangible warfare; the advent of radar.

The necessity to develop means for increasingly technologically-assisted warfare meant that the reliance on these capabilities similarly increased. When war again erupted in Europe in 1939, all major belligerents had already identified both the potential of the new unseen mediums of war, while similarly identifying the possibilities afforded in disrupting them. Radio communication had become standard issue for armour, infantry, navy and air forces seeking to operate massive forces jointly in relative harmony. Electronic navigational aids became crucial towards effectively directing large-scale assaults beyond enemy lines and prevent miscalculations. For the first time, impacting the adversary's freedom to operate in the electromagnetic spectrum became a priority.

The Second World War was a prolific exercise in counter-innovation embodied by constant attempts to jam adversary systems; it was the dawn of what would later be known as electronic countermeasures (ECM). As one of the pioneers of Western radar technology Robert Watson-Watt recounted, such secrecy shrouded this new set of capabilities that they often simply failed; operators were not aware of the value of their own missions and could barely practice in advance[183].

This caution to avoid unnecessarily publicising capabilities was not singularly exercised by British forces. Jammers operated by German forces were muted until absolutely necessary to assist a kinetic operation[184]. In 1942, a German naval battle group spearheaded by the battleships Scharnhorst and Gneisenau attempted to break the British blockade at Brest. Despite routine patrols by British aerial reconnaissance employing active radar measures, the battle group escaped initial detection. As an investigation would later reveal, The German ships enacted large-scale jamming operations once they set sail from port[185]. This in turn allowed the battle group to gain distance against its would-be pursuers, eventually allowing the ships to reach German ports. The jamming itself was not even particularly technically effective – it was by virtue of operational surprise that it achieved its results[186]. As Watson later recounted on the failure of British radar operators to discern German jamming from equipment failure:

> *"If I am held to my reiterated statement that radar is not merely an equipment or a group of equipments, but a system, then the radar system did fail but the electronics held out; the men behind the electronics were lamentably far behind*[187]*."*

[183] Robert Watson-Watt, "Battle Scars of Military Electronics - The Scharnhorst Break-Through," *IRE Transactions on Military Electronics* 1, no. 1 (March 1957): 19.
[184] Watson-Watt, 22.
[185] Cockburn, "The Radio War," 428.
[186] Cockburn, 430.
[187] Watson-Watt, "Battle Scars of Military Electronics - The Scharnhorst Break-Through," 24.

As critically discovered, there is a trust relationship between machines and the humans that operate them; operators must trust that the equipment functions as intended, and machines require that the operators use them correctly and appropriately act on their output. On one hand, operators of electronic countermeasures realised that they had little to assure them of their mission's success. Unlike the bullet or the bomb, getting confidence in measures that have no physical manifestation was a counter-intuitive process. The scientific research and development processes have indeed flourished and resulted in many potent and novel platforms[188]. However, operators of electronic equipment would at times lose faith in their capability to assess that it is indeed functioning as intended. Rudimentary radars and communications equipment frequently failed due to a host of operator and mechanical reasons. Adding jamming and adversary interference to the list of failures often meant a core loss of confidence in the capability itself[189]. It was often difficult to tell when a system was misbehaving, and if it was – why.

Improvements in communications were similarly pivotal to the war effort, both for the attacking and defending parties. Whereas wireless communications were gradually introduced in the First World War, by 1939 they have become pivotal for joint force operation, artillery targeting and range finding, and coordination of strategic effort. Reliance on radio signalling increased explosively. It was so meaningful that British research and development efforts resulted in an airborne communication jamming platform named *Jostle II*, that was subsequently used extensively in the Middle Eastern campaign. Jostle II was designed to disrupt communication networks employed by German tanks and armoured fighting vehicles (AFVs), which in turn affected their ability to operate in unison effectively[190].

Another key aspect of intangible warfare would emerge around the same time; it *is highly dependent on intimate familiarity with the adversary's equipment, systems and operational techniques*. Put simply, a great deal of high-quality intelligence collection was required in order to successfully fashion jamming or disruptive electronic countermeasures[191]. Each adversary device functioned and transmitted differently. Consequently, technology seeking to degrade the performance of these devices had to accommodate their idiosyncrasies and unique characteristics. Intelligence operations to detect, investigate and map equipment characteristics and vulnerabilities were key towards supporting the research and development processes of countermeasures and counter-countermeasures. It was a subtle and risky endeavour.

As a dangerous corollary, battlefield commanders and strategists realised that the dependency on jammers was a double-edged sword; *to use an electronic countermeasure risked losing it*[192] . In some cases, even limited recalibration, frequency changes or transmission modifications could thwart the effectiveness of jamming. This created a palpable tension between operational commanders who

[188] M. Fortun and S. S. Schweber, "Scientists and the Legacy of World War II: The Case of Operations Research," *Social Studies of Science* 23 (1993): 596–97.
[189] Cockburn, "The Radio War," 427–28.
[190] Cockburn, 429.
[191] Cockburn, 426.
[192] Cockburn, 429.

sought to increasingly wield these powerful new capabilities towards fulfilling their objectives and senior command, who had understandable concerns over compromising key intelligence sources. There was no easy solution to this issue and the uneasy balance remains to date. The Second World War thus marked the first conflict in which the considerations of intangible warfare grew dominant in the battlefield.

Finally, that an adversary's hardware could be remotely manipulated for effect proved to be the first indication of an underlying theme for all intangible warfare: *it is at its core an exercise at deceptively weaponising the adversary against itself*. Rather than seeking to directly impact the enemy, initial forms of jamming, spoofing and decoys sought to actively disrupt the operational decision-making process, in turn causing the adversary to act against its own stated goals. Borrowing from military strategist John Boyd's OODA Loop[193], intangible warfare graduated from disrupting the first observation phase to impacting the subsequent orientation, decision and actioning phases. While disruptive attempts were tactically possible prior to improvements in technology, influencing electronics has made the exercise possible at scale. Causing the myriad devices used in the battlefield to betray their operators quickly became a viable operational goal, a necessity to defeat the modern war effort. Thus, the Second World War had affirmed the need to invest heavily in technology for future conflicts rather than rely primarily on manpower and strategy. Indeed, an entire scientific field gradually emerged from the integration of new capabilities and the mathematical understanding of the battlefield – operations research[194].

Second Cycle – Cold War & Electronic Warfare

In 1973 and in spite of concrete intelligence prompting preparedness, Arab forces led by Egypt and Syria successfully attained strategic surprise by concurrently launching attacks against Israel in what would later be known as the 1973 Arab-Israeli War. In the first several days of combat, Israeli forces were beaten back from their strongholds in the Sinai desert and the Golan heights. Existing Israeli Defense Forces deployments met with freshly furnished Soviet technology in great numbers. Even as they encountered numerous difficulties on the ground and in the air, the Israeli military had within several hours proactively launched naval forays intent on engaging Soviet-made missile boats in use by the Syrian Navy. While seemingly a marginal series of battles, they would prove to be deeply prescient of a larger trend. The naval skirmishes included the first ever engagement to ever include guided ship-to-ship missiles, and the first engagement to effectively use ECM (Electronic Counter-Measures) to subvert guided missiles[195].

On paper, the odds were stacked in Syria's favour. The Soviet SS-N-2 Styx missiles used by the Syrian and Egyptian navies had twice the range of their 20-mile indigenous Israeli counterpart, the

[193] John Boyd, "The Essence of Winning and Losing," (June 28, 1995), http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf.

[194] Fortun and Schweber, "Scientists and the Legacy of World War II: The Case of Operations Research," 601–5.

[195] Robert S. Bolia, "Overreliance on Technology in Warfare: The Yom Kippur War as a Case Study" (DTIC Document, 2004), 53, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA485884.

Gabriel[196]. The Styx had been previously used even in the same theatre of war, when a volley fired from an Egyptian vessel sank the INS Eilat in late 1967, marking one of the Israeli Navy's greatest disasters[197]. This previous painful experience prompted Israeli missile boat captains to engage all forms of countermeasures upon establishing hostile contact, which included flares, anti-air gunfire and electronic radar spoofing. The aggressive posture when coupled with capably operated ECM and accurate guided missile fire proved decidedly effective. The Israeli Sa'ar 4 missile corvettes evaded or otherwise destroyed all incoming threats, while commensurately sinking five Syrian ships[198]. The strategic effect was significant even for a war with minimal naval aspects; Syrian ships were thereafter confined to their ports, and Israeli corvettes continued to harass coastal targets with impunity. The so-called Battle of Latakia had demonstrated that cautiously integrated intangible warfare can measurably augment operational efforts.

While the naval theatre proved a success for the Israelis, the airspace was not as easily dominated. Indeed, a presumption of superiority by the Israeli Air Force (IAF) has resulted in sorties against some of the world's densest anti-aircraft defensive spheres. In the first phases of the war, failure to employ ECM in order to contend with active surface-to-air platforms such as the stationary SA-6 Gainful or the mobile SA-7 Grail[199] resulted in staggering losses as the IAF rushed to provide air support and suppress advancing Syrian and Egyptian ground forces[200]. A lack of electromagnetic superiority proved costly. While the war itself had many consequences and several aspects of significance for warfare analysts, one such key aspect stood out most prominently; it was a war in which a prevailing overreliance on technology was thoroughly probed for vulnerabilities, and it was the first war in which the electromagnetic spectrum affected the war on a strategic scale.

A further interesting characteristic stemmed from the 1973 Arab-Israeli War and other Cold War era conflicts pitting US and Soviet technology; *intangible warfare has evolved in earnest beyond deceiving human operators to include deceiving the weapons themselves*. The increasing miniaturization of computers meant that greater automation could be relegated to the actual weapon platforms, thereby improving accuracy and response time while freeing operators to pursue mission-critical tasks. Communication networks to facilitate large-scale defensive operations and coordinate operations by disparate assets were becoming increasingly commonplace. These networks served as both a potent advantage while similarly resulting in a sizeable increase in the vulnerable attack surface. By falsifying signals, disrupting sensory input and affecting communication between devices, weapons could be manipulated beyond their original intent. And by attacking centres of gravity where electromagnetic defensive measures were concentrated for effective and prompt allocation of resources, one could palpably reduce an adversary's capabilities.

---

[196] Lawrence Whetten and Michael Johnson, "Military Lessons of the Yom Kippur War.Pdf," *The World Today* 30, no. 3 (March 1974): 109.

[197] Dov S. Zakheim, "The United States Navy and Israeli Navy: Background, Current Issues, Scenarios, and Prospects" (Center for Naval Assessment, 2012), 4, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA559163.

[198] Israeli Navy, "אתר חיל הים",1973 - מלחמת יום הכיפורים, accessed January 23, 2017, http://www.navy.idf.il/1274-he/Navy.aspx.

[199] Bolia, "Overreliance on Technology in Warfare," 51.

[200] Nadav Safran, "Trial by Ordeal: The Yom Kippur War, October 1973," *International Security* 2, no. 2 (1977): 151.

In 1968 and in light of dangerous liberalization of public sentiment[201], forces from the Soviet-led Warsaw Pact invaded Czechoslovakia. The surprise invasion included large-scale suppression of anti-air defences by way of electronic attacks, designed to prevent Czech command from obtaining situational awareness and scrambling whatever defensive measures were available[202]. The surprising and overwhelming show of electromagnetic force alongside the streaming of troops and armour into the country contributed to its relatively bloodless compulsion into submission, despite military resources being available to the Czech defensive. While largely non-violent widespread civilian unrest was pervasive[203], Soviet forces encountered no organized military resistance, possibly deterred at least in part by the overwhelming electromagnetic superiority. Intangible warfare became an independently strategic component when wielded in a coordinated fashion as a part of a joint warfare campaign.

The coalescing of doctrine around the electromagnetic spectrum soon gave birth to a precursor taxonomy to the one employed today in cyber-operations. In 1969, the US Joint Chiefs of Staff issued policy intended to clarify terminology around the use of electronic warfare. It was defined as:

> *"...military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum.*[204]*"*

Most interesting perhaps is just how similar this nearly fifty-year-old definition – dating from the earliest days of computing – to the manner in which cyber-warfare is framed today. Otherwise put, replacing both electromagnetic spectrum (the domain) with cyberspace and electromagnetic energy (the medium) with computer network equivalents retains the accuracy of the above definition perfectly. The guiding principles of intangible warfare have thus been codified in the same manner for at least fifty years, chipping somewhat at its perceived novelty.

Initially electronic warfare was divided into three key parts[205]. The first, electronic countermeasures (or ECM), was the prevailing term for measures designed to affect devices operating on the electromagnetic spectrum, mainly for communication and radar. As these measures proliferated, countries sought to defeat them by using the uninspired second term electronic counter-countermeasures (or ECCM). These defensive measures included frequency hopping transmitters to defeat jamming, and techniques designed to identify actual targets within chaff clouds. Lastly, the third component is electronic support measures (or ESM), a term which encompasses all operations and capabilities that enable ECM and ECCM. Otherwise framed, these are intelligence efforts on enemy electronics and electronic warfare capabilities. As previously mentioned and much like its

---

[201] Kieran Williams, *The Prague Spring and Its Aftermath: Czechoslovak Politics, 1968-1970*, 1st ed. (Cambridge, United Kingdom: Cambridge University Press, 1997), 3–6.

[202] U.S. DIA, "Soviet Electronic Countermeasures During Invasion of Czechoslovakia" (U.S. Defense Intelligence Agency, October 1, 1968), 1–3.

[203] Vanja Petkova, "Gen. Djurov's Report on the Participation of Bulgarian Troops in the Warsaw Pact Operation in Czechoslovakia, 30 September 1968" (Wilson Center, September 30, 1968), 3–4, Fond 1-B, Record 49, File 158, History and Public Policy Program Digital Archive, Central State Archive, http://digitalarchive.wilsoncenter.org/document/110014.

[204] Burton et al., *The Strategy of Electronic Warfare*, 1.

[205] Burton et al., 1–2.

modern cyber counterpart, electronic warfare is highly dependent on high quality intelligence. Both offensive and defensive capabilities must inherently be tailored to the adversary technology they're designed to affect.

The Cold War also saw the expansion of vernacular beyond countermeasures to proactive attacks. This initially included terms such as electronic attack (EA) and electronic warfare (EW). The increased integration of offensive electronic capabilities led to their recognition as not just reactive measures to attempt and defensively stymie an aggressor's momentum, but as a key component of joint warfare. As early as 1975, Soviet documents discussing large-scale military exercises began including a separate section on electronic warfare[206]. By 1977's Soviet Baltic Sea Exercise VAL-77, electronic warfare was identified as a key tenet of joint operations to be tested throughout combat trials[207].

As noted by Western observers, Soviet forces adopted an intangible warfare doctrine that rather closely mirrored its US counterpart, calling it Radioelectronic Combat (REC)[208]. Notably different, however, was the mathematical approach adopted towards its use. Recognising that it is far easier to recover and respond to REC efforts at degrading command and control, Soviet planners modelled adversary behaviour in order to identify its critical time windows. Those were reportedly defined as "the sum of times required to complete a sequence of steps in control[209]", or alternatively as the decision-making window for operational command. The goal of REC, therefore, would be to attack directly in that critical time window, as to disrupt crucial decision making and attain maximum impact.

Third Cycle – Command & Control

The strategic significance of computers and the networks they comprised increased at an explosive pace throughout the second half of the 20th century. The growth was largely commensurate with wider trends in computing; namely the increase in available computational power and storage volume, miniaturization, and declining hardware costs. Computers rapidly became more adept at handling additional aspects of the complex modern battlefield, and thus uniquely capable to facilitate large-scale joint operations and precision targeting. Military networks for communication, logistics, command and control, targeting, and telemetry became ubiquitous and progressively more connected. In countries where the development of joint warfare lagged, military observers noted Western progress with concern. Such was the case of the Soviet Union, which in its final years correctly identified its increasing military capability discrepancy with the West as partly a result of a woefully underdeveloped computer hardware industry[210].

---

[206] USSR Exercise Control Staff, "Task for the Operational Command Staff Exercise Soyuz-75 for the 4th Army" (Cold War International History Project, March 1975), 9, Polish Institute of National Remembrance, http://digitalarchive.wilsoncenter.org/document/113511.

[207] USSR Exercise Control Staff, "The Operational-Tactical Exercise of Allied Fleets in the Baltic Sea, Codenamed VAL-77" (Cold War International History Project, 1977), 13, http://digitalarchive.wilsoncenter.org/document/114599.

[208] U.S. Army, "U.S. Army Field Manual 100-2-1: Soviet Forces" (Headquarters of the Department of the U.S. Army, July 16, 1984), 178.

[209] U.S. Army, 178.

[210] Eliot A Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, no. 2 (1996): 39.

Saddam Hussein's refusal to vacate his forces from occupied Kuwait in 1991 had triggered one of the most prominent joint warfare campaigns to date. In Operation Desert Storm, accurate and concurrent firepower was brought to bear across all warfighting domains, all overseen and enabled by an expansive surveillance grid comprised of satellites, AWACS monitoring aircraft, ship-borne radars, allied facilities in the region and tactical equipment at the brigade level. The result was an overwhelming strategic success that reverberated globally, later hailed by some as a "revolution in military affairs[211]" (RMA). Global observers from militaries in Russia, China and others all noted the arrival of precision joint warfare on an unprecedented scale, crucially enabled by a sprawling Command, Control, Communications, Computers & Intelligence (or C4I) mechanism deeply woven into all operations[212].

This increasing reliance on networked warfare also signalled the deepening symbiosis between intelligence and combat operations. As former Director of National Intelligence James Clapper[213] wrote in 1994, Desert Storm revealed that the era of precision guided warfare created an insatiable need for intelligence[214]. In order for operations to proceed effectively, they now required additional coverage, available persistently before, during and after conflict, and it must be of higher quality. In this new world, adversary intelligence collection must be fully integrated across all domains of warfare[215].

In the 1990s, the United States– then the chief pioneer of intangible warfare under the new networked reality – evolved its military doctrine beyond the electromagnetic spectrum in its perception of intangible warfare. Namely, it now encapsulated its kinetic and non-kinetic efforts to influence the flow of information under a new umbrella term called *command and control warfare (*C2W). Initially, the term was in fact coined as command and control countermeasures, reflecting the innate tendency of intangible warfare in embodying counter-innovation [216]. Almost immediately, the term was reinvented as employing warfare vernacular[217]. Most importantly, the concept represented a doctrine comprised of five interlocking components:

> *"[Command and control warfare is] the integrated use of operations security (OPSEC), military deception [(MILDEP)], psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such action"*[218].

---

[211] Cordesman et al., *Chinese Military Modernization and Force Development*, 34.

[212] Norman B. Hutcherson, "Command & Contorl Warfare: Putting Another Tool in the War-Fighter's Data Base" (Alabama, United States: Air University Press, 1994), 1.

[213] At the time of the cited report, Clapper was the director of the U.S. Defense Intelligence Agency (DIA).

[214] James R. Clapper Jr, "Challenging Joint Military Intelligence" (DTIC Document, 1994), 94, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA528900.

[215] Clapper Jr, 40.

[216] U.S. Army, "Army Regulation 525-20: Command & Control Countermeasures (C2CM)" (U.S. Army Headquarters, July 31, 1992).

[217] Chairman of the Joint Chiefs of Staff, "Memorandum of Policy No. 30: Command and Control Warfare," March 8, 1993.

[218] Chairman of the Joint Chiefs of Staff, 2.

With C2W, Intangible warfare fully progressed beyond support capabilities weaved into the existing domains, instead becoming an operational goal of its own. C2W was a result of an increasingly ingrained understanding that modern command and control networks essentially formed new Clausewitzian centres of gravity. As US Army Field Manual 100-6, dated 1996, explains; "…C2W applies to all phases of operations, [and] offers the military commander lethal and non-lethal means to achieve the assigned mission…[219]". The very technology that was used to enable modern warfare has finally become a primary target instrumental in facilitating battlefield success. All five key pillars of C2W embodied a continuation of previous efforts at intangible warfare and a prescient look at modern-day cyber operations. Technological military deception (MILDEP) efforts woven into operations in order to create adversary false situational awareness were in place since the earliest days of radar-based ECM[220].

It was perceived that non-kinetic capabilities supported, enabled and empowered their physical counterparts in a larger holistic doctrine. The perception of intangible operations as intertwined with their kinetic counterparts was instrumental in implementing C2W; of its five pillars, only one (physical destruction) was inherently kinetic, while the others (EW, MILDEP, PSYOP, and OPSEC) had both kinetic and non-kinetic possibilities. Offensive electronic capabilities, much like their subsequent cyber counterparts, were viewed as a means to an end, particularly potent when combined intelligently with other available assets. In some cases, such as the US Navy's former Space and Electronic Warfare specialty area assessed to be analogous to C2W, intangible warfare was intrinsically pre-assumed to function alongside the traditional modus operandi[221]:

> *"The constant improvement of C2 and C2W systems alike tend to create a see-saw affect. As C2 systems are created with "anti-C2" fixes, C2W systems are developed to counter them. The lethality of Counter-C2 assets such as HARM [High-Speed Anti-Radiation Missiles] and sophisticated jamming modulations must continue to stay ahead of C2 systems upgrades*[222]*."*

The brief era of C2W was also accompanied by the realization that military intangible warfare is one component in a larger battle for information dominance. The notion of *information warfare* was gradually introduced as a contest for controlling the overall flow of facts and situational awareness before, during and after conflict. The concept later extended to operations conducted routinely even in neutral or allied territory, as part of the larger war of narratives. Intangible warfare had essentially spread beyond the military domain to aspects of grand-strategy. As stated in the US Joint Doctrine for Command and Control Warfare dated 1996, "Command and Control Warfare (C2W) is an application

[219] U.S. Army, "U.S. Army Field Manual 100-6: Information Operations" (Headquarters of the Department of the U.S. Army, August 1996), 37.

[220] Ron C. Plucker, "Command and Control Warfare - A New Concept for the Joint Operational Commander" (DTIC Document, 1993), 6, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA266700.

[221] Plucker, 16.

[222] Plucker, 21.

of [Information Warfare] in military operations… to attack or protect a specific target set – command and control (C2)[223]".

Considering that the US itself viewed C2W as tactically and operationally subordinate to larger information warfare efforts[224], it's no surprise that other countries do not make the distinction even today. Instead nations such as Russia, China, Iran and Israel view information warfare holistically, as a paradigm that envelops all operational levels including what's often called operations other than war (or OOTW). The holistic approach again indicates how artificial the distinction between cyber warfare and information warfare may be to some; one is contained within the other, the latter can often also be the former, and in many cases, they are implemented and operated by the same personnel. Thus, the notion of "cyber" as a distinct operational domain is similarly artificial, as cyberspace is merely the latest manifestation of the transfer and storage of information.

As everything today is data-based, information warfare extends to far greater reaches than it has before. Electronic warfare elicits tactical-level effects in an attempt to influence remote adversary hardware by way of the electromagnetic spectrum. Command and Control warfare, now largely an abandoned construct, indicates an operational-level doctrine originally designed to guide targeting against critical nodes to where information flows, analysed and subsequently disseminated as necessary. Strategic information warfare is the attempt to impact the flow of information beyond the scope of military operations, as to influence decision makers and the population they are entrusted with securing.

Fourth Cycle – Cyber Warfare and Information Operations

The rise *of* network centric warfare (NCW) in the 1990s was commensurate with the understanding that intangible warfare is difficult to accommodate as long as it is not practiced frequently and at scale. While the increased networking of military forces was already proceeding apace for several decades, doctrinal texts encompassing warfighting as a networked force reliant upon information technology were still lacking. As in many cases, NCW terminology was far ahead of its actual implementation. This was reaffirmed by US Department of Defense researchers in their surprisingly candid intro to the book *Network Centric Warfare*, dated 1999:

> *"The truth is that we are not experts on NCW and far more importantly, in our opinion, no one is. In fact at the current time, NCW is far more a state of mind than a concrete reality*[225]*."*

Secondly, network centric warfare further cemented the notion that the integration of information networks into warfighting did not constitute a radical departure from the underpinning tenets of

[223] U.S. Joint Chiefs of Staff, "Joint Publication 3-13: Command and Control Warfare (C2W)" (U.S. Joint Chief of Staff, February 7, 1996), 5.

[224] Plucker, "Command and Control Warfare - A New Concept for the Joint Operational Commander," 2.

[225] Alberts, Garstka, and Stein, *Network Centric Warfare*, 5.

warfare itself. While digital networks and an increased reliance on computing presented both new opportunities and various challenges, the reality of combat remained roughly the same[226].

The introduction of network centric warfare – and its equivalents as observed by global US adversaries – is an intriguing mirror image of offensive cyber-capabilities. Where NCW recognized the exponentially increasing use of information gleaned from disparate sources as a potential pivotal asset used by commanders[227], cyber-warfare commensurately recognized this new reality as an equally pivotal vulnerability. Noting the rise of network centric warfare, therefore, is critically important in mapping out new centres of gravity observed by its users.

The trend of technology-dependent warfare was not unique to Western militaries. Through careful dissection of the coalition-based Desert Storm operation, the Chinese People's Liberation Army (PLA) soon diverted considerable efforts to attempt and both counter American NCW while also harnessing its advantages locally. This notion was one of the key contributors to the modern Chinese doctrine of *local wars under conditions of informatisation*. Informatisation was the modern philosophy that stated that information must be harnessed, fused and wielded at scale to enable pursuance of all national objectives, both military and otherwise[228]. While military analysts previously deemed the PLA far behind their American counterparts at the time of Desert Storm, by 2013 US Department of Defense analysts observed an overwhelming emphasis in PLA drills on joint networked warfare[229].

The 1990s also introduced one of the final key components; that *intangible warfare fundamentally represents a contest for information superiority*. Military doctrine - ever vigilant over the need to visibly achieve objectives –became increasingly broad in its references to the significance of information itself. Intangible warfare began affecting more than just individual systems and streams of data; it influenced the overall perception of conflict itself. The 1940s saw the introduction of electromagnetic capabilities to influence specific systems. The 1970s saw the maturation of these approaches towards influencing localized platforms working in unison. The 1980s led to the graduation into abstract regional and global data networks. The 1990s led to the critical evolutionary step into influencing psychological decision-making processes and global public perception. Intangible warfare now encompassed a wider range of activities than ever before.

In November 1992, the US Department of Defense issued directive 3600.1 succinctly titled "Information Warfare", detailing definitions and responsibilities for the US information order of battle. Notably, the doctrinal document underpinned its policy section with the following opening text:

---

[226] Alberts, Garstka, and Stein, 7.
[227] Alberts, Garstka, and Stein, 12.
[228] Anthony H Cordesman, "Chinese Strategy and Military Power in 2014" (Center for Strategic & International Studies, November 2014), 122.
[229] Cordesman, 126.

"U.S. Armed Forces shall be organized, trained, equipped and supported in such a manner as to be able to achieve a distinct information advantage over potential adversaries in order to win quickly, decisively, and with minimum losses and collateral damage.[230]*"*

The transition in vernacular from information warfare (IW) to information operations (IO) was so rapid as to almost be unnoticeable. Within four short years, warfare was swallowed up as a subordinate element of a far more ambitious scope for "information operations"[231]. In December 1996 the Department of Defense reissued directive 3600.1 with a comprehensively altered opening policy statement suggesting a loftier agenda:

"The Department of Defense must be prepared for missions from peace to war-to include military operations other than war (MOOTW), such as peace-keeping and humanitarian operations, opposed by a wide range of adversaries including State and non-State actors. To meet this challenge, DoD activities shall be organized, trained, equipped, and supported to plan and execute [Information Operations]. The goal of IO is to secure peacetime national security objectives, deter conflict, protect DoD information and information systems, and to shape the information environment. If deterrence fails, IO seek to achieve U.S. information superiority to attain specific objectives against potential adversaries in time of crisis and/or conflict. The goal of IO is to promote freedom of action for U.S. forces while hindering adversary efforts.[232]*"*

While information operations were at least superficially far broader in scope, their core components bore a striking similarity to previous iterations of intangible warfare doctrine, namely Command & Control Warfare (C2W). To wit, numerous official US documents on IO enumerate its five core competencies as Electronic Warfare, Psychological Operations, Military Deception, Operations Security and Computer Network Operations. These five elements are nearly identical to their predecessor C2W equivalents, with the exception of removing physical destruction and replacing it with computer network operations. Cyber had merely replaced the last kinetic crutch in the broader spectrum of intangible warfare.

The latest iteration of intangible warfare marked the transition to a doctrine more reliant on achieving non-physical objectives. A dependency on data served as the recognition that control of information has generated a completely new set of strategic, operational and tactical goals. Each of the aforementioned five core competencies represented a conduit for shaping perception, situational awareness, and the decision-making process across all operational levels. Political scientist Joseph Nye weighed on the topic in 1996 when claiming that an "…information advantage can help deter or

[230] U.S. Department of Defense, "U.S. Department of Defense Directive 3600.01 - Information Warfare," November 1992, 1.

[231] Specifically, the revised Directive 3600.1 from 1996 defines Information Warfare as "IO conducted during time of crisis or conflict…".

[232] U.S. Department of Defense, "U.S. Department of Defense Directive 3600.01 - Information Operations" (U.S. Department of Defense, December 1996), 1–2.

defeat traditional military threats at relatively low cost[233]". Otherwise put, information had finally outstripped in importance the equipment and networks through which it was carried.

The transition to an information-led doctrine was not without its difficulties. The marrying of peacetime and wartime operations, the inclusion of computer network operations (CNO), the exclusion of physical destruction, and the inclusion of global perception management (PM) into scope all contributed to a marring of boundaries. For example, the US Information Operations Roadmap from 2003 proceeded to call for aggressive proactive psychological operations (PSYOPs), advocating for vast resources invested into offensive information capabilities both during conflict and peacetime[234]. At the same time, the document recognised that due to a potentially global reach of propaganda in the internet age, the quality and coherence of messaging must be improved significantly and coordinated with numerous agencies.

The 1990s also saw the birth of "cyber" as acceptable terminology, gradually increasing in prominence alongside the other established terms. Cyber-everything had seemingly sprung into existence within a few short years launching a trend that would accompany military affairs well into the 21st century. But the etymology of the word dates back to the 1940s, thereby charting a similar – albeit distinct – course through modern history. In essence, cyber represented the ever-increasing interaction and dependence of man and machine[235]; an apt phenomenon accompanying the realities of intangible warfare. This new family of terms came to roughly encompass the notion of targeting computers, devices, and the software that powers them. As such, while it gained in popularity, "cyber" as a term did not contribute any lucidity or specificity. One of the earliest and oft cited articles on the topic remains Arquilla and Ronfeldt's "Cyberwar is coming!", dated 1993[236]. Interestingly, while it is often looked upon with derision as alarmist and overreaching, considering the nascent state of publicly acknowledged intangible warfare it was rather prescient. Namely, the authors distinguished between two key terms; netwar and cyberwar. The former bears a striking resemblance to ongoing influence campaigns waged against Western governments, often attributed to Russia:

> *"Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it[237]."*

Cyberwar, now an oft-misused term, was similarly defined fairly well by the authors and mimics somewhat the modern Chinese approach:

> *"Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and*

---

[233] Joseph S. Nye, "America's Information Edge," *Foreign Affairs*, March 1996, 20, https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge.

[234] U.S. Department of Defense, "Information Operations Roadmap," 5–8.

[235] Thomas Rid, *Rise of the Machines: The Lost History of Cybernetics* (Scribe Publications, 2016).

[236] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993): 141–65.

[237] Arquilla and Ronfeldt, 28.

communications systems… It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not[238]*."*

Cyber-capabilities therefore epitomise the cyclical nature of intangible warfare. It is the counter-narrative to network centric warfare, a direct assault on the new centres of gravity created by the increased dependence of the modern combatant on complex networks of sensors and data streams. As information became pivotal to waging warfare, it almost immediately spawned a targeting reaction. This did not go unnoticed by the United States, which in 1998 formed a miniscule force tasked with defensive cyber-operations – the Joint Task Force-Computer Network Defense (JTF-CND). The task force increased in size and importance over several years, evolving to encompass additional responsibilities. In 2003, offensive cyber-capabilities became more widely acknowledged[239]. By 2005, the US military established the Joint Functional Component Command – Network Warfare (JFCC-NW), tasked with coordinating offensive network operations[240]. The significance of targeting and defending information networks has grown so rapidly that by 2007, then National Security Agency head General Keith Alexander claimed – "USSTRATCOM [United States Strategic Command] has also begun to develop tactics, techniques, and procedures and other concepts into cross-mission strike plans[241]." Network operations, both defensive and offensive, have increased in visibility and perception as to eventually merit the establishment of US Cyber Command (USCYBERCOM) in 2009 to "…conduct full-spectrum military cyberspace operations in order to enable actions in all domains…[242]" The two decades beginning with the 1990s saw an incredibly dynamic growth process for network capabilities within the United States military[243].

Cyber capabilities and information operations were codified into NATO and US doctrine as distinct but overlapping terms. "Cyber" was recognised as a catch-all term for the protection and manipulation of data and the digital systems that handled it. Separately, information operations encapsulated a far broader range of concepts and operational procedures, from wartime tactical operations to grand-strategy attempts at shaping adversary perception. Not all experts uniformly agree to this delineation. To wit, Dorothy Denning - a leading US information security researcher - published her seminal 1999 book titled "Information Warfare and Security" in which she essentially equated the crux of information warfare to hacking operations[244]. By doing so – and in congruence with Russian information operations doctrine – Denning supported the notion that all operations against digital data are a part of the same spectrum.

A Revolution in Military Affairs?

[238] Arquilla and Ronfeldt, 30.
[239] U.S. Department of Defense, "Information Operations Roadmap."
[240] Jeffrey Caton L., "Army Support of Military Cyberspace Operations" (Strategic Studies Institute, January 2015), 5–7.
[241] Caton, 8.
[242] U.S. Strategic Command, "U.S. Cyber Command (USCYBERCOM)," U.S. Strategic Command, September 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.
[243] Dan Kuehl and Leigh Armistead, "Information Operations: The Policy and Organizational Evaluation," in *Information Operations* (Washington D.C.: Potomac Books, 2007), 18–20.
[244] Denning, *Information Warfare and Security*.

Military cyber capabilities are neither new nor revolutionary. They are the latest incarnation of intangible warfare, the discipline of achieving objectives by targeting the technologies that enable modern warfare. Since the dawn of the twentieth century, societies have embraced computer technology and as such it became a viable target. Cycles of counter-innovation necessitated increasingly complex solutions, so machinery and equipment became both an asset and a crutch. When said crutch is successfully impaired, the warfighter stumbles and is rendered ineffectual. Cyber-warfare is thus merely the latest method of targeting military vulnerabilities.

The supposedly unique circumstances around attacking computer networks are as shown, not all that unique. The secrecy around capabilities and their use dates to the very genesis of electromagnetic warfare in the Second World War. The voracious dependency of computer attacks on high-quality, high-quantity intelligence can easily be rooted in the Cold War contest of ECM and ECCM. That intangible warfare is a contest for information dominance as an independent objective can be traced to the 1990s doctrine on command and control warfare.

Attacking networks is a combination and escalation of all known parameters of intangible warfare. As time passed and connectivity increased, both the circumstances and potential impact intensified. Where once jamming radar could generate a localised tactical effect, network attacks now potentially enable an adversary to completely thwart a theatre defence grid. Where transmission proximity was once needed, attacks can now potentially be carried out by distant troops from the comfort of their remote facility. But in order to generate this magnitude of effect, the need for omniscient, ever-present, and extensive intelligence resources has sky-rocketed.

With the exponentially increased levels of complexity of modern communication networks, the challenges of intangible warfare have similarly scaled. Such abilities are more brittle than ever, and guarded with fervour. Where once their discovery would mean eventual countermeasures of uncertain value, discovering modern deployed offensive capabilities can potentially ruin both years-long operations and the potency of the very weapons themselves. The defensive task has similarly become seemingly insurmountable and includes defending everything from civilian critical infrastructure to tactical battlefield satellite uplinks. Each such piece of equipment incorporates numerous hardware and software components developed internationally by a convoluted and largely opaque supply chain, making it a daunting task to certify that a system is truly uncompromised.

Cyber has finally pushed intangible warfare over the brink of domainhood because all the existing parameters have been intensified to the point where they can deeply impact warfare itself. Attacking devices and the data they communicate can have dramatic impact on achieving battlefield objectives. Where once they were peripheral, computers have now permeated through every facet of warfare. So, while cyber is an independent domain, it has only become so because of the unprecedented dependence of all other domains on data.

Offensive cyber capabilities are only the digital network aspect of the larger spectrum of information operations. Even as NATO members scramble to assemble fresh doctrine and strategy to combat within this supposedly new space, other nations have already recognised that a wider

approach is preferable. The insistence on differentiating cyber from both the other domains and other forms of information operations is intriguing; as shown, the United States itself had by now officially recognised the role of CNO (Computer Network Operations) as a component in the grander strategic literature on information operations. The role that network attack capabilities play in MOOTW far outstrips their utility in combat.

This historical analysis is by no means an exhaustive look at all military attempts at shaping the information battlespace; it was intended as a sobering look at the evolutionary nature of intangible warfare. Similarly, this analysis is limited in scope as network-attack capabilities are still in their operational infancy. As Russia, China, the United States, North Korea, Iran, Israel and others rush to signal their willingness to operate militarily in networks, the efficacy of these operations remains to be gauged. The relative dearth of real-life, war-time military network attacks does not however prevent critically examining the historical processes that led to modern doctrine.

Cyber-warfare is the latest incarnation of the counter-innovation cycles characterising the modern battlefield. Countering radio with jamming has evolved into countering digital command and control with network attacks. Remediating the advantages of radar has advanced to compromising theatre-wide sensory awareness by targeting the network-centric mindset. The underlying logic is the same, but the modern reliance on networking has enabled its application on an ever-greater scale. The historical lessons of cyber-warfare are therefore that its true uniqueness stems from its unprecedented reach, sophistication and scope, not from it truly being a new domain of warfare.

3. Offensive Network Operations[245]

Overview

Offensive network operations epitomise the desire for cleaner, less violent conflict. If strategic coercion can be achieved by targeting the digital infrastructure used for both national security needs and daily life, enemy resolve should theoretically decrease to the point of surrender. This perception of conflict is understandably appealing, were it accurate. The notion of precluding violence by achieving digital supremacy is promising but has thus far yet to materialize. Instead, MONOs can assist both tactical and strategic combat efforts, if all their particular advantages and disadvantages are accounted for. While nations occasionally advertise slivers of information of how they conduct MONOs, doctrine and strategy remain understandably murky on how operational success is achieved in cyberspace. Having examined what constitutes cyber-warfare (see Chapter 1), and how intangible warfare evolved into modern offensive network operations (see Chapter 2), a third component can now be addressed; what are the unique characteristics of offensive network operations carried out by military forces?

At the core of this chapter is the argument that *MONOs can mostly be grouped into two classes; presence-based and event-based***.** Presence-based operations encompass any offensive network activities which include a lengthy intrusion component meant to establish a persistent foothold inside adversary assets, traverse networks and locate objectives. Event-based operations primarily include direct attacks intended to cause immediate effect against a targeted platform, by compromising its integrity or available resources. Most publicly acknowledged network intrusions would fall into the former category, while many direct attacks against military hardware in the battlefield would fit the latter.

A typology for network warfare matters. By identifying the two primary categories in which it applies to warfare, each category can be separately examined. When researched together, the results often seem muddled and difficult to translate to military doctrine. Examined separately, presence and event-based operations are shown to have distinctive characteristics embodying unique advantages and disadvantages. They require different manpower, resources, operational approaches, and can be applied against different targets for varying effects. Some may be more easily relegated to battlefield use, while others are best kept for strategic manoeuvres.

Event-based operations are roughly analogous to firing a weapon. When such an attack is launched a digital payload – a stream of data - traverses one or more networks where it meets or bypasses

[245] This chapter was published and presented at the 2018 CyCon X conference. The text of the publication is preserved, with an expanded introduction and conclusion, and additional case studies woven as complete paragraphs, as required for congruence with the rest of the thesis and its overall quality. Published parts of the text have only been modified for necessary format variations. For the original publication, see Daniel Moore, "Targeting Technology: Mapping Military Offensive Network Operations," in *2018 10th International Conference on Cyber Conflict (CyCon)* (IEEE, 2018), 89–108.

adversary defences. Impact on the target, if successful, is immediate or near-immediate. Such capabilities are meant to be reusable. An event-based attack may be launched by a local fire team (e.g. infantry), a warfighting platform (e.g. aircraft or surface ship), or altogether from remote territory (e.g. by a combatant command centre). These types of attacks – like their kinetic counterparts – often have localised impact meant to augment or support kinetic strikes. As a corollary, such tactical network warfare works well in a combined arms package, jointly deployed alongside kinetic capabilities.

Presence-based operations are roughly analogous to clandestine sabotage operations. A prerequisite lengthy intelligence operation results in access to the adversary's networks. From that point, the attacker's assets are manoeuvred to enumerate enemy servers and endpoints, gathering information and identifying weak points that may subsequently be attacked for effect, all the while evading defences. Specialized implants are fielded where needed, with the intent to activate when the order to do so arrives. The potential risk to friendly weapons and capabilities from discovery is far greater due to the extended presence "behind enemy lines", as is the chance of failure. But the potential benefit is commensurately immense, possibly resulting in an advantage of strategic proportions. These operations may serve as the surprise prelude to an offensive campaign, a one-shot capacity to degrade an adversary, or as a supporting means of exerting pressure on enemy governments in conflict.

Military network operations are discussed often but vaguely. On the defensive, many of the techniques employed by military forces are a product of publicly available information security best practices and industry standards. However as some of the characteristics of military networks deviate markedly from their civilian counterparts, defensive doctrine also differs. Despite these circumstances, a decade of widely publicised coverage on nation-state hacking operations, when coupled with leaked documents from the US intelligence community afford a partial yet meaningful glimpse into how offensive units can and do operate in cyberspace.

This chapter offers a deconstruction of MONOs for both event-based and presence-based attacks. The opening includes a review of existing approaches on the processes that define nation-state network operations, particularly focusing on public-sector and private-sector models used to assess network intrusions. The model chosen as the theoretical scaffolding for the chapter is the US Department of Defense's "Common Cyber Threat Framework[246]", which capably aggregates different industry and public-sector models to provide a useful approach for assessing wider network campaigns rather than focusing on individual intrusions.

The four primary phases presented in the Common Cyber Threat Framework – *preparation, engagement, presence* and *effect* – are assessed in order for both presence and event-based operations. *Preparation* includes all efforts to craft offensive capabilities, research enemy defences, and gather targeting intelligence. *Engagement* refers to the first contact with the adversary networks,

[246] U.S. DNI, "A Common Cyber Threat Framework: A Foundation for Communication."

the original point of intrusion and compromise. *Presence* refers to all actions carried out while malicious software is present on enemy networks, primarily to facilitate further compromise of assets, gather intelligence on the target and position implants for attack. Finally, *effect* entails the activation of the intended payload, which would then disrupt, degrade, destroy or otherwise adversely impact the targeted enemy asset. Not all network operations fall neatly into these four categories nor is the model fully representative of all activities associated with such operations. It does however offer a useful standard mechanism through which to analyse and compare the primary components of a broad range of different network attacks.

Responsibility for counter-intelligence traditionally lies with domestic law enforcement and intelligence agencies. Classically, there was little that the average citizen could or would do. Private intelligence firms more commonly restricted their spheres of influence to corporate espionage or criminal cases. Wary of retribution and unaware of political context, unaffiliated citizens would most often avoid wilfully involving themselves with the clandestine affairs of nations. In the internet age, that is demonstrably no longer the case. Private individuals and organisations frequently interact or even disrupt intelligence gathering efforts. Daily friction between private entities and nation-state adversaries has never been higher.

In early 2013, American cybersecurity company Mandiant published an extensive analysis of a perceived nation-state cyber-espionage campaign[247]. They had dubbed the phenomenon of a lengthy, targeted network intrusion by a capable adversary an "advanced persistent threat" (APT). Unusually for the time, the private company conducted complete adversary attribution for the operation. Mandiant called the group "APT1" and pointed the attribution finger at China. Incredibly, they went further and identified the responsible party to be the People's Liberation Army 3rd General Staff Department (3PLA), and even provided the specific unit indicator, 61398 – and the building in which it allegedly resided[248]. Several individuals were also directly revealed.

Mandiant understandably felt compelled to explain the unusual decision to meddle in the affairs of nations. In their APT1 report, the company authors exclaimed that "It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively[249]". While many other security companies have since shied from outwardly attributing intrusions to specific nations and organisations, detecting similar nation-state operations has become a wildly successful and largely consensual practice[250]. In some cases, companies such as the Moscow-based Kaspersky Lab have even taken to publicly outing malicious network activity undertaken by their host countries[251], thereby exposing themselves to possible

[247] Mandiant, "APT1 - Exposing One of China's Cyber Espionage Units," 2013, 1.
[248] Mandiant, 3.
[249] Mandiant, 6.
[250] Not all companies have shied away from granular attribution. As recently as August 2018, US company CrowdStrike has attributed an intrusion campaign they labelled "Stone Panda" to specific individuals and buildings in China. See Adam Kozy, "Two Birds, One STONE PANDA," *CrowdStrike Blog* (blog), August 30, 2018, https://www.crowdstrike.com/blog/two-birds-one-stone-panda/.
[251] GReAT, "'Red October' Diplomatic Cyber Attacks Investigation," *Kaspersky Securelist* (blog), January 14, 2013, https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/.

government retribution. For the first time in history, interfering in intelligence operations had become a viable business model.

The information security industry's new predilection towards tampering with network operations affords unprecedented transparency to how these now play out. The tempo of state-affiliated intrusions has increased, and private security companies have been remarkably successful at repeatedly unmasking them. As private companies assisted victims in mitigating and defeating network incursions by military units and intelligence agencies, the models, methodologies and techniques they have for doing so correspondingly improved. Thus, the information security industry and community expertise have become the best sources of publicly-available knowledge for analysis of state network operations.

Several industry models provide fragments of insight into assessing MONOs. In 2011, American security contractor Lockheed Martin published a paper outlining a model for assessing, mitigating and defending against network intrusions[252]. Borrowing from military vernacular, they originally labelled the new model the Intrusion Kill Chain[253], later colloquially renaming it to the Cyber Kill Chain[254]. The model provided a systematic, simplified process in which intrusions were deconstructed to seven chronological phases. A second popular network-intrusion analysis model is the Diamond Model[255]. Developed by veteran information security researchers, the model's four vertices (hence the diamond namesake) are *adversary, capability, infrastructure,* and *victim*. The wider notion behind the model is to assess intrusions by understanding the intruder rather than focusing on the victim. While these models – and others[256] – are frequently used by both private and public entities, they focus only on the technical and operational efforts in network operations. As such, they lend themselves more naturally to their intended technical audience rather than a strategic analysis of overall MONO capability.

The inherently secretive nature of cyberspace operations does not mean that there are no official publications on the topic. Predominantly, numerous sanctioned United States Department of Defense documents are immensely helpful in understanding official perspectives on how offensive network operations are conducted. The reports run the gamut from tactical accounts on how units operate on the field[257], joint publications on doctrine[258], strategic guidelines[259], oversight reports[260], and even

---

[252] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): 80.

[253] Hutchins, Cloppert, and Amin, 4.

[254] "Cyber Kill Chain," Lockheed Martin, accessed June 4, 2017, http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html.

[255] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intrusion Analysis" (DTIC Document, 2013), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA586960.

[256] See also the MITRE Corporation's ATT&CK Framework, used to assess technical characteristics of malicious network activity across the different operational phases. MITRE, "MITRE ATT&CK," 2018, https://attack.mitre.org/wiki/Main_Page.

[257] Sean Kimmons, "Cyber Teams Throw Virtual Effects, Defend Networks against ISIS," United States Army, February 15, 2017, http://www.army.mil/article/182400/cyber_teams_throw_virtual_effects_defend_networks_against_isil.

[258] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," May 2, 2013.

[259] Chairman of the Joint Chiefs of Staff, "National Military Strategy for Cyberspace Operations" (Chairman of the Joint Chiefs of Staff, December 2006).

[260] U.S. Department of Defense, "Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF)."

operational integration roadmaps[261]. While parts of the content remain redacted within these publications, when carefully amalgamated they become incredibly helpful.

By some estimates, over thirty countries are actively pursuing offensive cyber capabilities as a strategic goal[262]. Some nations – such as Israel – are notoriously tight-lipped when it comes to their integration plans. Others, such as Russia, China, and most so the United States discuss their strategies more liberally. Deterring nations in cyberspace is difficult; whatever nations can do to signal one another that they too can strike through this supposedly new medium may thereby prove useful. So, publicly acknowledging at least some form of offensive network operations may be a viable deterrence play.

Military Offensive Network Operations

The history of intangible warfare shows that investing time and resources into a weapon that may strike a single target once could still be a cost-effective decision. Others may be developed strategically to be made routinely available to battlefield units. How would these processes look? What forces, procedures, and relationships would that entail from inception to deployment? These are questions that are mostly left unhandled by existing industry models - which while useful - focus on assisting defenders in understanding and foiling targeted attacks. Expanding on these existing models allows accounting for additional processes undertaken in a military context. Among these research and development cycles, support intelligence gathering, tasking, and infrastructure management. Employing effective cyber operations is a grand undertaking; models assessing these processes should reflect that reality.

For the purpose of this thesis, the term military offensive network operations (MONOs) is used as the conceptual anchor. The term was previously defined as *any means of digitally affecting adversary systems and networks for a military goal or objective*. Military denotes a focus on non-civilian or law enforcement use of activities. Offensive limits the aperture to hostile engagements rather than information operations or intelligence collection. Network specifically focuses the scope on attacking software and hardware rather than information in a broader sense. Operations signifies a purposeful employment of capability in the scope of organised military activity.

When approaching the issue from a broad perspective, all network operations can be reduced to four critical parts: intelligence, capabilities, operators, and infrastructure. Intelligence represents all information gathering and assessment required to conduct effective operations against a given target. This includes prioritising adversary networks for targeting, analysis of used technologies and identification of exploitable vulnerabilities. Capabilities include all software and hardware components employed by the attacker to breach the target and influence targeted systems. The operators are the actual individuals deploying the tools and manipulating them as necessary. The

[261] U.S. Department of Defense, "Information Operations Roadmap."
[262] James R. Clapper Jr, Michael S. Rogers, and Marcel Lettre, "Statement on Foreign Cyber Threats to the United States," § Senate Armed Services Committee (2017), 5.

infrastructure is the amalgamation of virtual logistics necessary to effectively communicate with the target, maintain operational security, exfiltrate information, and control the tools being used. While some simple, limited operations can be carried out without one of the above components, any meaningful offensive manoeuvre will almost certainly have all.

MONOs do not exist in a vacuum. In contrast to some existing models, operations do not begin with reconnaissance against the target and do not end after acting on the objectives[263]. While the Kill Chain model reconciles the existence of multiple intrusion efforts that may run parallel against different targets within a given campaign[264], additional considerations are not within the scope of the model. There are several strategic and tactical phases preceding the operation itself, and several that follow it. Similarly, there are processes that run concurrently to a network intrusion, interacting with work carried out by network operators to facilitate their success and feed off of it. These additional components are not peripheral; they are instrumental to an operation's success and are an integral part of understanding offensive military capabilities in cyberspace.

The model used in this chapter expands on the Department of Defense's Cyber Threat Framework model to include all processes and stakeholders associated with a network operation's success. The goal is to reflect all requisite efforts by broadening the aperture to include intelligence providers, strategists, research and development, software engineers, and kinetic warfighters. Additional stakeholders and phases are assessed in each one of the model's four consecutive steps; preparation, engagement, presence, and effect.

The *preparation* step entails all prerequisite processes necessary to generate viable operational capacity. This includes oft ignored but substantial investments in research, development, initial targeting and strategic intelligence gathering. It is impossible to generate an effective attack without knowing what to attack, how to attack it, and have the integrated capabilities to carry out the attack. The *engagement* phase is the initial contact with the adversary networks, in which forward defences are subverted and initial compromise established. This original intrusion vector serves as the anchor for all subsequent malicious activity against the target. The third phase – *presence* – includes incremental infections of other subsystems within adversary networks, hunting for the objective while collecting pertinent intelligence. This step's duration ranges from possibly months or even years to a matter of seconds for event-based attacks. In the fourth and final *effects* phase, offensive payloads are activated against the target, hopefully resulting in the intended effect. This phase includes all post-attack procedures, such as folding back the attacker's infrastructure, covering up forensic evidence and conducting attack damage assessments.

In 2010, Iranian engineers submitted a request to the Belarusian information security company VirusBlokAda to assist them in investigating an incident[265]. It had seemed that malicious software had

[263] Hutchins, Cloppert, and Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 4–5.

[264] Hutchins, Cloppert, and Amin, 7–8.

[265] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *WIRED*, July 11, 2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

infected some of the computers and servers at the Natanz nuclear facility, part of the illicit Uranium enrichment program then operated by the Iranian government. They were not aware at the time, but they had stumbled on a clandestine offensive network operation intent on causing physical damage to the plant's centrifuges[266]. The malware was soon discovered to have specifically targeted the industrial control systems orchestrating the plant's operations[267], subtly masking its own activities as to fool local technicians into believing that physical centrifuge failures caused by the malware were accidental[268]. The offensive toolset, named Stuxnet by the researchers who discovered it, soon became the analytical cornerstone for offensive operations[269]. For the first time, malicious software employed was used by one state to kinetically target another. Some hailed it as the dawn of cyberwarfare[270].

Stuxnet was unique. As researchers scrambled to dissect the malware and its many characteristics, it became evident that its uniqueness was both a blessing and a curse. On one hand, researchers were afforded unprecedented intimate access to a thoroughly engineered, complex, targeted instrument of offensive state network operations. On the other, it was one of a kind, which immediately begged the question of how representative was it as an attack with a physical outcome. Stuxnet was likely a result of a complex network operation, requiring extensive investment in research, development, adversary simulation and a sensitive targeting cycle. While not used for a military objective, it was perhaps used to preclude one. Therefore, it remains a highly instructive example of a large-scale presence-based operation.

PREPARATION

Preparation encompasses all efforts preceding contact with the enemy. The Cyber Threat Framework defines preparation as all collective efforts to identify targets, develop capabilities, assess victim vulnerability, and define the scope of the operation[271]. Each of these processes reflects months and perhaps even years of investment in resources both material and operational. Thus, while it is the least discussed, the preparation phase of any offensive network operation may often be its longest.

Before operators ever interact with adversary networks, planners must first initiate a *targeting* cycle. This may seem deceptively trivial; an actor seeking to target an adversary will simply pursue its networks. In reality, locating, identifying and enumerating relevant networks for attack can be difficult [272]. Modern militaries employ dozens of disparate networks even within a single organizational entity[273]. Identifying which one to attack is no negligible feat. It requires in-depth intelligence and an understanding of the adversary order of battle. In many cases, sensitive or

---

[266] Zetter.
[267] Langner, "Stuxnet - Dissecting a Cyberwarfare Weapon."
[268] Falliere, Murchu, and Chien, "W32.Stuxnet Dossier," 3.
[269] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."
[270] Sharon Weinberger, "Is This the Start of Cyberwarfare?," *Nature* 474, no. 7350 (2011): 142, http://search.proquest.com/openview/8558e1d85b80b4fabe7a8ae1ae79704b/1?pq-origsite=gscholar&cbl=40569.
[271] DNI U.S., "Cyber Threat Framework Lexicon" (Office of the Director of National Intelligence, 2013), 2.
[272] Matthew Monte, *Network Attacks & Exploitation: A Framework* (Indianapolis, IN, USA: John Wiley & Sons, Inc, 2015), 20.
[273] Jack L. Burbank et al., "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology," *IEEE Communications Magazine* 44, no. 11 (2006): 39–42.

operational networks do not interface directly with the public internet or perhaps even with any other networks[274]. This makes the notion of identifying them and attaining access that much harder. The force commander will choose to pursue a target through networks only if it is deemed to be the most effective means of attaining the objective[275].

Targeting has an instrumental role that does not begin in cyberspace. Rather, targeting is "the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities[276]." But whereas in kinetic targeting it may be sufficient to simply know the location of the target, it is not the case for targeting virtual capabilities. The process entails both enumerating all relevant networks, identifying those which would potentially be prudent to target, and subsequently prioritising between those.

Targeting cycles are decidedly different for presence and event-based operations. Targeting for presence-based operations is most commonly conducted by the strategic intelligence entities that hold network intrusion capabilities. Traditionally, it is within the remit of signal intelligence (SIGINT) organizations, which in varying jurisdictions are either civilian or military entities[277]. As such, it is often a derivative component of those entities' prioritized intelligence requirements (PIRs). PIRs form a fundamental national security agenda against which the agency is expected to action, whether by collecting intelligence or preparing for eventual network attacks[278]. Targeting is therefore a long-term process in which intelligence on the adversary is accumulated, increasingly providing information required to properly prioritize between networks which are a balance of compromise feasibility and relevance to the objectives at hand. The result is a highly curated list of specific targets.

Strategic targeting cycles may require expert external assistance. In NSA documents leaked by Edward Snowden in 2013, cooperation efforts from 2004 between the NSA and the Defense Intelligence Agency (DIA) are described[279]. The DIA's Joint Warfare Support Office assisted in mapping and analysing materials about an alleged Russian military base buried deep in the Yamantau Mountain. As indicated in the document, the US intelligence community remained in the dark despite information on the facility first surfacing over a decade earlier[280]. The DIA asset helped targeting efforts to identify Russian entities associated with the project, marking them for subsequent signals intelligence collection[281] – and potentially network operation – efforts. Prioritisation and identification of the operational target was thus jointly determined by the two agencies.

[274] The idea of separating a network from all other networks is called "air-gapping", and is a widely accepted methodology of reducing a network's potential attack surface.

[275] Paul Ducheine and Jelle van Haaster, "Fighting Power, Targeting and Cyber Operations," in *6th International Conference On Cyber Conflict* (IEEE, 2014), 313–14, http://ieeexplore.ieee.org/abstract/document/6916410/.

[276] U.S. Joint Chiefs of Staff, "Joint Publication 1-02: DoD Dictionary" (U.S. Department of Defense, May 2017), 234.

[277] In the United States, the NSA is a civilian agency. In the Israeli example, it is the military unit 8200.

[278] U.S. Joint Chiefs of Staff, "Joint Publication 2-0: Joint Intelligence" (U.S. Department of Defense, October 22, 2013), 24–25.

[279] NSA, "SID and DIA Collaborate Virtually on Russian Targets" (National Security Agency, May 18, 2004).

[280] Michael R. Gordon, "Despite Cold War's End, Russia Keeps Building a Secret Complex," *The New York Times*, April 16, 1996, sec. World, https://www.nytimes.com/1996/04/16/world/despite-cold-war-s-end-russia-keeps-building-a-secret-complex.html.

[281] NSA, "SID and DIA Collaborate Virtually on Russian Targets."

Targeting for event-based operations would reasonably take place in proximity to the attack itself[282]. As a result, this cycle could commonly be conducted by the theatre force commander, or perhaps even a tactical unit lead against a limited objective. This alongside the employment of pre-packaged network capabilities entails that the decision-making process is both faster and conducted with far less available resources. In order to identify which networks should be selected for subsequent engagement, the commander must identify local adversary centers of gravity, which if compromised would reduce enemy effectiveness. To accomplish this, local reconnaissance assets conducting spectrum analysis and automated network mapping procedures may identify adversary networks operating in the region, possibly even auto-assigning possible ordnance to activate against them.

Some targets may be chosen for both event and presence-based operations, reflecting varying goals and opportunities. Over the last two decades, the United States has gradually modernized battlefield connectivity for its deployed forces. A part of this process, titled Warfighter Information Network – Tactical, or WIN-T, is a prime example of how saturated the network landscape can be. A combination of dedicated line-of-sight radios and satellite-communication terminals[283] services a host of networks including the general-purpose NIPRnet, SIPRnet[284] and local compartmentalized data and voice networks[285]. Many of these networks enable unclassified, ancillary functions that are not mission critical. Others carry sensitive targeting information, communication, or intelligence data. Some of these networks may be inaccessible as they are transmitted over a medium for which the attacker has little hope of gaining access. Others rely on commercial satellites and even the public internet as the transmission medium of choice. Completing the targeting process by successfully classifying which networks both matter and are pragmatically reachable is therefore a challenging commitment. In some cases, these networks may be subjected to a long-term compromise in the form of a presence-based operation. In other cases, locally accessible datalinks such as a regional network cell might be the target of an event-based attack. Interestingly, the WIN-T project has now been officially terminated by the U.S. military, citing concerns that the project's architecture is indeed too vulnerable to a determined, well-resourced adversary[286].

One crucial pre-operation process often overlooked is *capability acquisition and development*. Capabilities in network warfare include all hardware and software used to intrude, exploit, and affect enemy platforms. There is some limited merit in downplaying the complexities of this process; unlike actual weapons, network intrusion tools can ostensibly be developed by anyone. Similarly, the development cycle for a potent offensive network capability is also classically deemed to be much

---

[282] Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 2017, 181–82.

[283] Gregory Coile, "WIN-T SATCOM Overview Briefing" (Program Executive Office Command Control Communications-Tactical, 2009), 5.

[284] Non-Secure Internet Protocol Router Network (NIPRNET) and Secure Internet Protocol Router Network (SIPRNET), U.S. Department of Defense networks used for unclassified and classified communications between and within partner organisations.

[285] Lynn Epperson, "Satellite Communications Within the Army's WIN-T Architecture" (Program Executive Office Command Control Communications-Tactical, February 6, 2014).

[286] Bruce T. Crawford, James J. Mingus, and Gary P. Martin, "The United States Army Network Modernization Strategy," § Committee on the Armed Services (2017), 6–8, http://docs.house.gov/meetings/AS/AS25/20170927/106451/HHRG-115-AS25-Wstate-CrawfordB-20170927.pdf.

shorter[287], easier, and cheaper[288]. Again, there is some reason to this assertion. However, the unique circumstances of developing weaponry to attack networks are well worth examining. Network weapons are often frail, specific, and difficult to reliably test.

Presence-based attack tools must be stealthy, agile, and modular. They must be stealthy as the majority of their life-cycle will be spent clandestinely embedded in adversary networks. They must be agile as to enable operators to creatively use them to traverse adversary networks, collect intelligence, and weaponize valuable targets. Finally, they often must be modular as to allow operators to only deploy necessary capabilities at any given moment, thereby reducing the footprint of the tool – a further operational security mechanism[289]. Each deployment of a highly engineered network attack tool must be carefully managed as to only include the components currently needed to facilitate success. The expectation that presence-based operational tools be stealthy introduces a significant weakness; these tools become quite brittle to use. The pervasive notion that offensive network tools are single-use stems from this very issue[290]. The defensive cycle for a network adversary is demonstrably shorter, as detected malware can result in detection signature within days of its discovery by a capable defender. It is not just the particular deployment that is threatened, detection of an offensive platform risks its compromise against all targets against which it is currently employed. That is a momentous risk of capabilities, which explains in part why intelligence agencies often guard them so emphatically.

The McDonnell-Douglas F-15 Eagle aircraft first entered service in the United States in 1976[291]. Originally designed to counter the Soviet Mig-25 Foxbat, its role exponentially grew with its exemplary service record to include additional missions. Despite significant Soviet developments in fielding newer aircraft and air defences, the F-15 continued to receive upgrades to its avionics, weapons, radars and targeting subsystems[292]. Adaptations and newer models such as the F-15 Strike Eagle meant that the same platform could retain its utility even against modern threats. As a result, it remains a highly active warfighting platform both domestically and internationally, and is expected to continue its active service at least until 2025[293]. This means that that the F-15 will have a total of at least fifty years of active service.

It is almost inconceivable to envision network attack tools enjoying the same operational longevity as their kinetic counterparts. One of the longest known offensive network operations platforms - codenamed Regin by its private-sector discoverers - was ostensibly operating since at least 2003[294]

---

[287] Rattray, *Strategic Warfare in Cyberspace*, 171.
[288] Nye, "Cyber Power," 5.
[289] Monte, *Network Attacks & Exploitation*, 124.
[290] Libicki, *Cyberdeterrence and Cyberwar*, 83.
[291] David R. King and Joseph D. Massey, "History of the F-15 Program: A Silver Anniversary First Flight Remembrance" (AIR FORCE LOGISTICS MANAGEMENT AGENCY GUNTER AFB AL, 1997), 11, http://www.dtic.mil/docs/citations/ADA328680.
[292] John A. Tirpak, "Making the Best of the Fighter Force," *Air Force Magazine* 90, no. 3 (2007): 44, http://www.airforcemag.com/MagazineArchive/Documents/2007/March%202007/0307force.pdf.
[293] Tirpak, 44.
[294] Kaspersky Lab, "The Regin Platform: Nation State Ownage of GSM Networks," November 24, 2014, 3.

and widely attributed to the NSA[295]. At the time of its discovery in 2014, security company Kaspersky claimed that it was "…one of the most sophisticated attack platforms we have ever analyzed[296]". Once publicized and with its various mechanisms for communication and stealth thoroughly mapped and defended against, NSA operators would have had to immediately cease all intrusion activity until sufficient changes could be made and new evasion mechanisms deployed. Such an event is both an enormous investment in time and resources and also a potentially major operational compromise. It would be as if one successful loss of an F-15 to an S-300 air defence battery would cause the immediate grounding of all F-15 aircraft globally – even against other adversaries - until such a time as countermeasures could be developed, tested and deployed for the entire fleet. It is clearly not the case.

Conversely, event-based attack tools must be robust, aggressive, fool-proof and intuitive to operate. As they would likely be deployed by frontline units, no expertise must be needed to wield them effectively. They must be able to operate against a wide range of targets in a slew of contingencies, while generating similarly predictable effects. Battlefield operators will not have time to dynamically redeploy modules or carefully orchestrate network traversal. The weapon must therefore be capable of autonomously completing its objectives without further assistance. As a result, resource exhaustion attacks such as the commonly seen denial of service or generic destructive payloads are apt examples of preparing event-based capabilities.

Both presence and event-based capabilities require investment in *vulnerability research*. This entails all efforts to locate exploitable flaws in software and hardware used by the adversary, flaws that can be subverted for compromising the target and getting it to either behave unexpectedly or preferably run arbitrary code. Vulnerability research runs the gamut from generic-use software such as Microsoft Windows to dedicated software use by military hardware and other niche platforms. It is a crucial component in most network attack tools.

Some vulnerabilities are more useful than others. In August 2016, an entity calling itself the Shadow Brokers began releasing information seemingly pilfered from the NSA's then network intrusion unit, Tailored Access Operations (TAO)[297]. Assessing the potential fallout from the significant compromise of some of their most compartmentalised capabilities, the NSA decided to attempt and pre-empt any damages that may occur from having their most sensitive attack tools repurposed against others. They disclosed to Microsoft that they have previously discovered a critical vulnerability affecting multiple versions of their Windows operating system[298]. The vulnerability was the holy grail of intruders; it allowed remote code execution (RCE), and it was "wormable". Thus, it

[295] Marcel Rosenbach, Hilmar Schmundt, and Christian Stöcker, "Source Code Similarities: Experts Unmask 'Regin' Trojan as NSA Tool," *Spiegel Online*, January 27, 2015, sec. International, http://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html.

[296] Kaspersky Lab, "The Regin Platform: Nation State Ownage of GSM Networks," 23.

[297] Dan Goodin, "Group Claims to Hack NSA-Tied Hackers, Posts Exploits as Proof," *Ars Technica*, August 16, 2016, https://arstechnica.com/information-technology/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/.

[298] Ellen Nakashima and Craig Timberg, "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did.," *Washington Post*, May 16, 2017, sec. Technology, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

could surreptitiously infect additional vulnerable computers with ease. Quite simply, it was a virulent vulnerability.

Duly alarmed, Microsoft quickly released a patch for the vulnerability. Coding it MS17-010, the company strongly advised all its customers to quickly patch their systems or risk extreme vulnerability to external compromise[299]. Many did so, and many more did not. Two months later, a tidal wave of ransomware infections swept across the world severely impacting users both large and small. Interestingly, it appeared that the malware - dubbed WannaCry by researchers - weaponised the MS17-010 vulnerability by way of the Shadow Brokers leak[300]. Among other fragments of information, the Shadow Brokers leak provided the internal NSA name for MS17-010 – EternalBlue. The effects of the malware were staggering; some organisations such as the UK's National Health Service suffered greatly from the malware, resulting in temporary loss in operational capacity[301]. Seemingly it could have all been prevented had they patched their aging internal systems.

WannaCry was later attributed both officially by the US and the UK government and unofficially by private sector researchers to the North Korean government. It was a stark reminder that even disclosed vulnerabilities may retain their potency, particularly against targets that are difficult to routinely patch and defend. Even WannaCry itself was insufficiently severe to encourage all Windows users to inoculate against EternalBlue. Less than six months later, a second wave of infections from the Petya malware once again weaponised the same vulnerability to a surprising degree of success[302].

Are WannaCry and Petya representative of the modern networked battlefield? Likely not - most military networks are segmented from the internet and are comparatively more resilient. Yet WannaCry and its brethren are instructive in one key area; effective vulnerability research is paramount to the success of a reliable network attack platform. This requires the expert attention of vulnerability researchers who comb through the source code of products used in adversary networks and systems. If a weapon is detected and made public, losing a powerful vulnerability can be a crippling loss as inoculation becomes near imminent for many modern networks and devices. Similarly, public disclosure of a vulnerability used in weapons means it cannot reliably be used in sensitive operations again, even with different tools being deployed. The risk of discovery becomes too great.

Software vulnerabilities are difficult to find both for attackers and defenders. From the offensive perspective, effectively exploiting critical software in a manner conducive to intrusions is increasingly difficult[303]. At the same time, there is no shortage of vulnerabilities, as data indicates that publicly

---

[299] Microsoft, "Microsoft Security Bulletin MS17-010 - Critical," Microsoft, July 14, 2017, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

[300] Symantec, "What You Need to Know about the WannaCry Ransomware," Symantec, October 23, 2017, https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

[301] National Audit Office, "Investigation: WannaCry Cyber Attack and the NHS," National Audit Office, accessed January 1, 2018, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

[302] Symantec, "Petya Ransomware Outbreak: Here's What You Need to Know," October 24, 2017, https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper.

[303] Symantec, "Internet Security Threat Report" (Symantec, April 2017), 16, https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

disclosed, high severity submissions have nearly doubled in 2017[304]. From the defender's perspective - as a RAND report indicated in 2017 - unless the tool weaponizing them is somehow discovered, vulnerabilities last an average of almost seven years without being exposed[305]. Thus, maintaining an expert workforce entrusted with continuously hunting for new useful vulnerabilities is paramount.

For event-based operations, the final component of preparation is integrating capabilities for use with forward-deployed warfighting platforms. Presence-based operations are often handled by remote operators, much like drones. However, in many cases, especially those involving segregated networks used to communicate sensitive data, proximity or line-of-sight access is required. In these cases, military forces may find themselves delivering fires directly in the field, be it by aircraft, naval vessel, ground vehicle or actual boots on the ground.

There are recent examples of event-based attacks in which network capabilities were supposedly integrated into battlefield platforms. The United States military operates infantry cyber teams to work alongside electronic warfare assets to map out enemy networks and identify targets[306]. The Russian military has allegedly disrupted Royal Air Force sorties over Syria by way of a network attack launched from a deployed electronic warfare vehicle[307]. Developing a reliable, robust, battlefield-deployable offensive cyber capability is increasingly becoming viable – albeit expensive. Thus, while attacking networks may seem to be low-cost, attaining battlefield readiness and conducting event-based offensive operations may include hefty development, targeting, and intelligence cycles.

ENGAGEMENT

Network operations are not carried out solely by operators. Even once attack capabilities are fully developed, vulnerabilities weaponised, and targets identified, extensive support from other functions is essential in order for an operation to succeed. Therein lies a difficulty in applying the cyber kill chain model directly to military operations; much of the work is not carried out by the operators themselves. Those who facilitate the attack will likely need subject-matter assistance from intelligence analysts, reverse engineers, software developers, and decision makers.

The Cyber Threat Framework defines the initial engagement phase as "Threat actor activities taken prior to gaining access but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores[308]". Put simply, this phase embodies the attempts to intrude upon the enemy; it is the first active contact with its networks, intent on establishing a digital beach-head. What the framework obfuscates is the characteristics of this phase. As adopted from the operational typology used by Buchanan, the

[304] NIST, "NVD - CVSS Severity Distribution Over Time," NIST, 2017, https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time.

[305] Lillian Ablon, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits.* (Santa Monica: RAND Corporation, 2017), 11.

[306] Kimmons, "Cyber Teams Throw Virtual Effects, Defend Networks against ISIS."

[307] Giannangeli, "Russians 'Hacking into' RAF Crews over Syria."

[308] U.S., "Cyber Threat Framework Lexicon," 4.

engagement phase may occur months in advance for presence-based operations or in adjacency to the desired effect, as for event-based attacks[309]. Not all cases are created equal, but all share one notable commonality - the engagement phase starts the operational clock.

For presence-based operations, network operators in the engagement phase are mainly conductors, overseeing the weaving of other orchestra members' capabilities into the operation. They are thus reliant upon external assistance for success. Intelligence analysts are most familiar with the target and would likely be best positioned to pair an intrusion approach to it. Technical staff may be required to assist in selecting the appropriate payload to defeat enemy defences and evade detection. Senior staff may be necessary to prioritise goals as the operation proceeds.

A ubiquitous approach to network intrusion is compromising an internet-facing server or device. Identifying and compromising these may be easier than directly penetrating segregated networks, but not all such targets are inherently useful. Operations may also commence by interacting with an individual rather than a machine. Strategic network operations intent on gaining entry to sensitive networks may first need to compromise those who routinely use them and hold trusted access to their assets. The reason for this is two-fold; first, there may not be a viable technological intrusion vector, as many sensitive networks are cut off from external inputs. Second, the users are often the most vulnerable element in an otherwise secure network[310]. They are prime targets for social engineering as an intrusion vector, but that does not mean it is always a trivial endeavour. Successfully getting individuals to usefully compromise their own security without arousing suspicion often requires expertise, preferably provided by dedicated personnel.

Even defence contractors can be compromised by social engineering. In march 2011, the RSA security division of US company EMC reported a breach of its networks[311]. RSA soon admitted that the intrusion vector consisted of a phishing email containing a weaponised spreadsheet. As per the company's then head of security, "the email was crafted well enough to trick one of the employees…[312]", thus admitting the attackers into the network. Yet the effects had a far wider reach, as RSA was also the producer of the SecurID tokens used for authenticating access in many government contractors and agencies. Indeed, it was revealed two months later that defence giant Lockheed Martin – prolific designer and manufacturer of US military equipment – was targeted in part by counterfeit SecurID tokens created as a result of the RSA breach[313]. Securing presence on both RSA and Lockheed Martin networks was therefore a fairly long and involved process.

---

[309] Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*, 76–84.

[310] Neil Barrett, "Penetration Testing and Social Engineering: Hacking the Weakest Link," *Information Security Technical Report* 8, no. 4 (2003): 56–64.

[311] John Markoff, "SecurID Company Suffers Security Breach," *The New York Times*, March 17, 2011, sec. Technology, https://www.nytimes.com/2011/03/18/technology/18secure.html.

[312] Uri Rivner, "Anatomy of an Attack," *Speaking of Security - The RSA Blog* (blog), April 1, 2011, https://blogs.rsa.com/anatomy-of-an-attack/.

[313] Christopher Drew, "Lockheed Says Hacker Used Stolen SecurID Data," *The New York Times*, June 3, 2011, sec. Technology, https://www.nytimes.com/2011/06/04/technology/04security.html.

In event-based operations, the engagement phase can occur in seconds. As the targeting cycle is similarly shortened, there is no time to craft phishing emails tailored to human targets or set up elaborate honeypots. Instead, the engagement phase will focus on compromising accessible targets by exploiting remote software and hardware vulnerabilities. Particularly when using automated capabilities to target warfighters or other connected devices, it is sometimes possible to directly attack the software to gain entry. The engagement phase for event-based operations may not always result in full access to the target. Depending on what the desired effect is, it simply may not be necessary. For example, simply attempting to exhaust available resources or corrupt a target's means of communication may be possible without ever being able to execute code directly on the target. If the goal is to prevent the target from functioning as intended, that may be sufficient. Such scenarios are more easily placed within a military context; see for example denial of service attacks, which bear some similarities to conventional electromagnetic jamming[314].

The potential perpetrators for event-based operations are far more varied than their presence-based counterparts. In many cases, these could be forward deployed offensive cyber units, as both the U.S. and the U.K. are increasingly using[315]. In other instances, field staff such as human intelligence assets or specific warfighters may be required to facilitate the actual engagement. As Edward Snowden revealed in a leaked top-secret document in 2013, the NSA's GENIE program to facilitate semi-automated network operations would at times rely on such assets. When necessary, field operators would physically infect adversary devices, plant hardware, or conduct short-range offensive SIGINT[316]. SIGINT agencies with global or regional reach could also deliver payloads from remote facilities.

PRESENCE

The presence phase is where most of the friction occurs between intruder and target. It is where persistent malicious software is continuously employed to understand, dissect and establish a hold within the targeted network or networks, gradually extending the intruder's access until such a time where it locates servers or devices fitting to attain the task at hand [317]. It is therefore the process of extending and cementing the reach into the adversary's networks, two processes called lateral movement and persistence, respectively. As defined by the Cyber Threat Framework:

> *"[The presence phase includes] actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at*

[314] This aligns nicely with U.S. military doctrine that situates Cyber and Electromagnetic Activities (CEMA) as a unified operational function, see U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities.".

[315] U.S. Army, 30–32.

[316] NSA, "Computer Network Operations - GENIE," 2013, https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf.

[317] U.S., "Cyber Threat Framework Lexicon," 5.

will against the host physical or virtual computer or information system, network and/or data stores[318]*."*

The presence phase embodies the biggest discrepancy between the two operational categories - time spent in target. Where presence-based operations unsurprisingly spend most of their lifecycle in the presence phase, event-based operations may either have an inconsequential or perhaps even non-existent presence phase. When nation-state intrusion campaigns are analysed and reported to take months prior to detection, it primarily refers to the presence phase. The key difference in timespan reflects applicability to two wholly different operational tempos. For presence-based operations, the presence phase is essentially a cyclical process of expanding micro-intrusions in which additional nodes in the network are scanned, breached and subsequently assessed for mission relevance. This is represented well in the Kill Chain model, which threads multiple compromises on targeted networks into a single campaign with shared features[319]. Each intrusion must be handled with care as to avoid tripping any alarms or informing network defenders of an active intrusion against them.

Networks are comprised of multiple servers, computers, and other devices. It is usually unfeasible for an attacker to attain its objective via the first node breached on the network. As a corollary, upon gaining entry, the intruder would then proceed to perform what is often called "lateral movement". Such procedures are meant to establish presence on the network, infect additional nodes, and try to locate targets of worth for further assessment. While operating the software to facilitate these endeavours is squarely within the purview of the operators, they require tremendous amount of support from intelligence staff[320] to assess content pulled from devices and servers, while research and development resources may be required to create dedicated modules to subvert specific technologies encountered.

Presence-based offensive operations are first intelligence operations. Until such a time as a more active measure is needed, malicious software is tasked with either remaining dormant or collecting information, identical to its behaviour in an intelligence mission[321]. As a corollary, operators at the presence phase must rely extensively on the assistance of intelligence analysts to assist in further targeting and dissection of materials exfiltrated from the target[322]. In some cases, the offensive is carried out wholly by the intelligence agency[323]. The presence phase is thus both assessing the independent intelligence value of the target, while simultaneously gathering information needed to help steer the operators towards the server or servers where attacking would result in achieving the desired objective.

When Russian operators initially infiltrated the Ukrainian power grid in 2015, they did not immediately wreak havoc on all they encountered. Instead, earlier intrusion efforts cleverly used the

---

[318] U.S., 5.

[319] Hutchins, Cloppert, and Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 7–8.

[320] Jeff Malone, "Intelligence Support Requirements for Offensive CNO" (August 23, 2010).

[321] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4 (2010): 64.

[322] Malone, "Intelligence Support Requirements for Offensive CNO," 16.

[323] GCHQ, "Full-Spectrum Cyber Effects" (GCHQ, 2012).

specialized protocols unique to these industrial networks to traverse the network, map its layout and glean information required to develop robust offensive capabilities[324]. In a subsequent operation, the presence phase included pivoting from the power company's corporate network onto its industrial network, leveraging an attack against both to simultaneously cripple the grid and prevent operators from fixing it[325]. Finally, advancements eventually allowed the operators to "…de-energize a transmission substation on December 17, 2016[326]" by way of the CRASHOVERRIDE malware tailored to impact even relatively well defended energy grids. The Russians had achieved a malware-induced blackout, but they have done so after a considerable amount of time from the initial engagement phase. Success would not have been possible without topical expertise and accrued experience.

Success would not have been possible without topical specialty. As reported, the operation revealed a command of the industrial communication protocols at use, a rapidly evolving sophisticated malware platform with dedicated modules, and politically relevant targeting all the while dodging detection by wary defenders. These circumstances embody the intricacy and difficulties of successfully traversing the presence phrase. It would not have been possible without technical expertise in industrial control systems, developers to generate the unique modules, and intelligence support to guide the efforts.

Regardless of how secure the target is, the physical consequences of failure are hardly comparable to a botched kinetic attack. Much like the motivations behind operating drones over contested airspace, this is a key advantage of offensive network operations. Indeed, even at the absolute worst scenario in which the offensive measure both fails and results in a catastrophic compromise of the attacker's capabilities, the actual operators are certainly to remain free from physical harm. They are distant, often operating from the safety of their homeland, and as such will be untethered to physical harm concerns. They will be able to rebuild and attack another day[327].

For event-based offensive operations, the presence phase is nearly imperceptible. This is intrinsic to the attack vector; capabilities employed in an event-based attack are meant to impact the target directly and then disappear, leaving as few lingering artefacts as possible. Were tell-tale indicators to remain such as residual code left running or files persisted to the target's file system, it would simplify subsequent efforts by the adversary to develop future countermeasures. Thus, it is significant for an event-based capability to be only minimally present on enemy assets.

A cascading effect – intentional or otherwise - may result in an event-based attack having a limited period of network presence. For example, an automated network attack tool designed to propagate through networks and rapidly destroy all infected endpoints and servers would require a limited presence as to ensure subsequent infections to additional targets. A good example of such an attack is the NotPetya destructive malware, which in 2017 heavily affected Ukrainian networks before

[324] Dragos, "CRASHOVERRIDE: Threat to the Electric Grid Operations," 9.
[325] Dragos, 10.
[326] Dragos, 4.
[327] Monte, *Network Attacks & Exploitation*, 63.

cascading beyond its scope to adversely impact various other entities globally[328]. The attack, which resulted in extensive damage to victims worldwide, was unusually publicly attributed by numerous Western intelligence agencies to the Russian military[329].

The potential cost incurred in discovery is arguably the most meaningful deterrent to attacking via cyberspace. In recent years, a growing trend amongst large vendors in the information security market has been to uncover massive nation-state surveillance efforts, those often facilitated by highly sophisticated malicious software. The immediate result of this compromise is an attempted rollback of all deployed assets both by the original offender attempting to effect damage control and the victims who enjoy updated configurations for their defensive products. The product of this is both a partial collapse of the aggressor's intrusion infrastructure but more importantly – the defender's near-immediate inoculation from future attempts to use the same tool in an offensive capacity. The presence phase is thus the most sensitive component in many offensive network operations. The continuous friction with different adversary networks and the need to collect intelligence means that discovery and eventual inoculation are a big risk to attackers. Presence operators therefore must continuously work to conceal their moves, clean up forensic evidence, and establish stable, covert communication channels that would reliably enable decision-makers to activate positioned offensive payloads once these become necessary[330].

Effect

The final effect phase is where triggers are pulled. Ordnance is activated, disabling, disrupting or manipulating targets. Effects either translate into objectives, fizzle uselessly, or have unintended and potentially disastrous collateral impact. For presence-based operations, the effect phase is the culmination of possibly months of planning, targeting, intelligence collection, infection attempts and dedicated development[331]. For event-based operations, the effect phase represents the primary thrust of the attack. When Richard Clarke declared in 2009 that "strikes in cyber war move at a rate approaching the speed of light[332]", he referenced not the entire span of an operation but rather the span of time between the activation of the ordnance to its actual detonation against the target; the manifestation of the effect phase. Even so, ordnance may be instantly triggered but may still take time to achieve its intended impact.

Distilling various official definitions, there are three "attack" types when targeting networks – disruptive, manipulative, and destructive[333]. Disruptive - or suppressing - attacks incur "temporary or

[328] Nicole Perlroth, Mark Scott, and Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," *The New York Times*, June 27, 2017, sec. Technology, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

[329] See for example U.S. Press Secretary, "Statement from the Press Secretary."

[330] Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies* 36, no. 1 (February 2013): 123.

[331] Rattray and Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," 79.

[332] Richard A. Clarke, "War From Cyberspace," *The National Interest*, 2009, 32.

[333] Adapted from the U.S. Military's taxonomy of "…deceive, degrade, deny, destroy, or manipulate…", see U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities," 17." Libicki similarly speaks of attacks meant at eruption (target illumination), disruption, and corruption. See Libicki, *Cyberdeterrence and Cyberwar*, 145.

transient degradation by an opposing force of the performance of a weapon system below the level needed to fulfil its mission objectives[334]". Their utility increased with the rise of electronic warfare, where electromagnetic transmissions could be jammed to produce a temporary but potent effect[335]. Disruptive attacks have made a natural transition to cyberspace, where temporarily degrading the capacity of military resources can adversely impact the efficacy of an adversary force[336].

Disruptive network attacks are commonplace even outside military scenarios. So-called denial-of-service attacks capable of levying massive throughput of network traffic routinely disrupt the functionality of online services big and small. The targets range from global gaming communities such as Sony PlayStation Network[337] to major banks[338]. Typically, these attacks either exploit an implementation flaw in the targeted technology or simply attempt to overwhelm its available resources. By doing so, no legitimate connections can interact with the platform as intended, rendering it temporarily disabled for its original purpose. Similar approaches may be applied to military technology, platforms, and protocols.

Manipulation effects attempt to alter information or functionality in the adversary networks, thereby deceiving operators or preventing intended system functionality. Such attacks attempt to alter perception, preventing an adversary from acting properly to further its own objectives. A scenario could include introducing a nearly imperceptible deviation to a weapon's targeting process, causing strikes to miss by what could appear to be a technical glitch. Kinetically, this is hard to accomplish but could be roughly analogized to physically tampering with a missile's warhead to secretly render it inert. When the missile fires, it seemingly behaves as normal until impact, during which the warhead does not detonate. During the heat of conflict and until it happens repeatedly and consistently, it would be difficult to identify the fault as an attack. By the time it is discovered, it would likely already be too late. As the Stuxnet campaign demonstrated[339], masking a manipulative effect to increase its longevity can cause an effect to be repeatedly successful over time. Hiding an effect does, however, require incrementally introducing it; an immediate and blunt change of circumstance markedly increases the probability of detection.

Masking an effect may be more applicable to presence-based operations than to event-based attacks. As previously discussed, event-based tools tend to be more geared towards instantaneous effects and are thereby less compatible with the subtle machinations of a presence-based effect. Conversely, as event-based capabilities are designed to be more resilient to detection, it is perhaps less

---

[334] U.S. Joint Chiefs of Staff, "Joint Publication 1-02: DoD Dictionary," 229.

[335] Army Headquarters, "US Army Field Manual 3-13 - Information Operations," November 2003, 7.

[336] U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities," 9.

[337] Sarkar Samit, "Massive DDoS Attack Affecting PSN, Some Xbox Live Apps," *Polygon*, October 21, 2016, https://www.polygon.com/2016/10/21/13361014/psn-xbox-live-down-ddos-attack-dyn.

[338] Jasper Hamill, "Bank-Busting Jihadi Botnet Comes Back To Life. But Who Is Controlling It This Time?," *Forbes*, June 30, 2014, https://www.forbes.com/sites/jasperhamill/2014/06/30/bank-busting-jihadi-botnet-comes-back-to-life-but-who-is-controlling-it-this-time/#3df4bb0f6f07.

[339] Falliere, Murchu, and Chien, "W32.Stuxnet Dossier"; Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."

paramount for an effect to be so hidden. It would be surely preferable, but not a requirement per se of the attack.

Destructive attacks are aimed at inflicting damage on adversary networks, either on hardware, software, or both. These types of attacks are firmly rooted in conventional warfare, where destruction of enemy assets and personnel is often seen as the primary method of reducing its coercive combat effectiveness[340]. When applied to network operations, a destructive attack could cause permanent software damage – such as in the case of malware which completely erases all critical files on target servers[341], or even permanent hardware damage, such as the previously mentioned Stuxnet worm targeting the Iranian nuclear project[342].

One of the key challenges in the effects phase of a presence-based operation is that the attackers do not hold the trigger. A presence-based operation is about painstakingly wiring ordnance into enemy assets, infecting endpoints and servers as relevant networks are identified and penetrated. However, when the time comes to activate the payload, there is no confidence that the attack will be correctly registered and actioned upon by the infected machine slotted to do so. Unlike kinetic or even event-based attacks, the weapon is effectively embedded behind enemy lines when it is fired. The offensive payload is already pre-placed within adversary networks, increasing the chance that the triggering itself would fail due to some extrinsic circumstance outside of the attacker's control.

The other side of the reliability issue is conducting effective battle damage assessment (BDA), the process of estimating the effects of an attack. This difficulty applies to both categories of operations, with some key delineation. Primarily, issues stem from a lack in visible confirmation. Excluding rare cases, intangible warfare normally has no physical aspects in its effects phase. Software is manipulated, hardware may be fooled or tampered with, but physical safeguards designed to protect equipment and operators from faults may often prohibit such drastic effects. This is of course not always the case. Presence-based incidents such as the centrifuge-crashing Stuxnet[343], the generator-rupturing Aurora experiment[344], and the German steel mill attack[345] remain among the few instances of significant physical damage to equipment directly caused by a software attack. Physical impact is immensely hard to accomplish.

---

[340] The classic approach to warfare - most commonly codified by Prussian strategist Carl von Clausewitz – favours destruction as the sole means of achieving military coercion. See chapter 4 for the application of this principle to cyber-warfare, or Clausewitz, *On War*. for the original school of thought.

[341] See for example the 2012 Shamoon attack, in which a presumably Iranian attacker wiped thousands of computers at Saudi's national gas company, Aramco; Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (May 2013): 81–96.

[342] Langner, "Stuxnet - Dissecting a Cyberwarfare Weapon."

[343] Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."

[344] The "Aurora Experiment" was a 2007 showcase by the Idaho National Laboratory in which they demonstrated how a software vulnerability in generators used by critical infrastructure providers can rapidly cause physical damage to the point of complete equipment destruction. The experiment video and associated documentation is available online as "Operation Aurora," MuckRock, July 3, 2014, https://www.muckrock.com/foi/united-states-of-america-10/operation-aurora-11765/#files.

[345] The German steel mill attack is a 2013 incident in which attackers supposedly caused significant physical damage to a furnace by way of a presence-based operation, see Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack" (SANS ICS, 2014)..

A destructive event-based attack with no discernible BDA means that it is often challenging to assess whether the target has in fact been degraded, either permanently or temporarily. As with other characteristics, this outcome ambiguity is similar to electronic warfare. Thus, if as previously suggested the goal of the network attack was to facilitate a subsequent kinetic manoeuvre, operators may be forced to make a leap of faith that the attack has indeed been successful. In some cases, this leap may entail risking lives. Gambling on whether a software attack successfully degraded an anti-aircraft targeting radar's sensors to the point where manned fighters are safe to engage is a high-stakes endeavour.

Network attacks are intrinsically detrimental to their own BDA efforts. Kinetic attacks are often accompanied by sensors. These provide crucial telemetry as to the success of an attack, and can include manned solutions such as special forces, submarines, or aircraft, or unmanned solutions such as drones or satellites. For presence-based operations, the attack tools are often their own sensors. Indication as to the status of the targeted system or network may singularly come from that very system or network. Take down the network and crucial observation channels similarly disappear. For networks, it is usually only possible to conduct effective surveillance by observing the data coming in, out, and through the network. The activation of an earnestly crafted presence-based destructive attack may cut off all such communication, taking with it the ability to observe whether the desired effect had actually been accomplished.

Challenges and Opportunities

Delineating between event-based and presence-based operations allows having a discussion on how militaries are integrating these capabilities into doctrine and strategy. Both are markedly different in characteristics, duration, challenges, and opportunities and thus must not be lumped together. Fundamental similarities exist between the two categories and are certainly helpful towards understanding networks as a medium for warfare; but useful observation of military capabilities will remain limited unless we recognize that not all capabilities must be treated the same.

Event-based operations represent the instances in which network attacks are somewhat analogous to the kinetic. Like firing a weapon, an event-based operation entails sending a payload from attacker to target in the hope of immediately reducing its integrity or capacity to operate. As a result, these capabilities are often more tactical in nature, easier to integrate with existing military OODA loops[346], and are promising candidates for joint warfare. They are however limited in scope, may require extensive research and development, and could be limited to a specific subset of adversary equipment. A weapon suitable for disabling a U.S. Navy destroyer may exploit hardware-specific vulnerabilities[347] rendering it unsuitable against other targets. Consequently, battlefield operators deploying such

[346] OODA loop – A process in which combatants Observe, Orient, Decide, and Act. Military vernacular for conceptualising decision-making process in combat. See Boyd, "The Essence of Winning and Losing."
[347] These vulnerabilities indeed exist, see for example U.S. Department of Defense, "Aegis Modernization Report Program - Fiscal Year 2016" (U.S. Department of Defense, 2017), 3.

weapons must have immaculate understanding of their adversary and a firm control of their own options.

Presence-based operations are intelligence missions with an offensive finisher; a form of digital sabotage. They may initially appear indistinguishable as operators infect networks and gather information necessary to craft an attack. In these phases, even if the target detects the malware present in its assets, it is immensely difficult to assess motive and intent. Only once offensive modules are deployed can confidence in hostile intent increase. This adds an unfortunate layer of political nuance, as overly successful network intrusions may be misconstrued by the target as unduly aggressive. The risk of potentially undesired escalation has been aptly covered by Buchanan when discussing the "cybersecurity dilemma"[348], an application of the classic security dilemma to network intrusions between nations.

Presence-based operations can potentially be high-risk, high-reward capabilities. Successfully pre-positioning assets in military or otherwise critical networks may potentially have meaningful impact on the course of conflict if used to facilitate strategic surprise or large-scale reduction in enemy capacity to operate. At the same time, presence-based operations are notoriously brittle, and their discovery can undo years of focused labour. By nature, such operations require tight, intensive, unyielding support of friendly intelligence assets to map the threat, generate initial persistent access, and successfully manoeuvre through inscrutable tangles of military networks until the relevant targets are found. It is therefore understandable why these campaigns are often spearheaded by intelligence with core expertise on network intrusions rather than deployed military forces.

The Lockheed-Martin F-35 Lightning II fighter aircraft is a fascinating example of a platform potentially vulnerable to both presence-based and event-based attacks. After two decades of development, the aircraft had started active deployment accompanied by a host of issues with its onboard software. These included major in-flight failures of the radar system[349], issues with its onboard avionics[350], and "…276 deficiencies in combat performance [designated] as 'critical to correct'…[351]". Additionally, both the onboard systems and the logistical software used to manage the F-35 have demonstrated numerous vulnerabilities during security testing procedures, many yet to be addressed as of 2017[352]. While onboard systems are unlikely to be directly connected to the internet[353], targeting one or more of the F-35's prized array of sensory inputs and communication methods is viable by a knowledgeable adversary. To that end, evidence suggests that the F-35's most recent software version still presents a sizeable attack surface.

An event-based attack might try to overwhelm or otherwise compromise some of the F-35's tactical data links, used to share data with allied assets in the air and on the ground. For compatibility

[348] Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*.
[349] Gallagher, "F-35 Radar System Has Bug That Requires Hard Reboot in Flight."
[350] U.S. Department of Defense, "Fiscal Year 2015 DoD Programs - F-35 Joint Strike Fighter (JSF)," 35.
[351] U.S. Department of Defense, "Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF)," 48.
[352] U.S. Department of Defense, 103–4.
[353] Lin, "Offensive Cyber Operations and the Use of Force," 66.

purposes, this communication commonly occurs via the Link-16 protocol, an encrypted legacy protocol used by NATO forces since 1975. While it has undoubtedly undergone improvements over its lifecycle, the limitations in encrypting reliable airborne tactical traffic and the vast array of opportunities for U.S. adversaries to intercept, analyse and exploit Link-16 protocol vulnerabilities raise the option that it may be compromised during an attack. Link-16 includes targeting information, location of friendly forces and directives from command forces[354]. Interestingly, even oversight reports have indicated some issues with the Link-16 data that forced pilots to revert to voice communication [355]. Others have indicated intermittent problems with the Multifunction Advanced Data Link (MADL) system used to communicate between fifth generation stealth aircraft[356], causing pilots to "…lose tactical battlefield awareness [357]". Successfully compromising the F-35's data links is thus not unfeasible and may severely degrade aircraft battlefield performance.

The effects phase in this particular instance could include one of several options. As an example, a manipulation attack could alter the pilot's perception of the battlefield by adding, removing, or moving specific targeting points fed to the radar subsystem by external channels. A disruptive attack could alternatively try to overwhelm sensory input, or prevent the aircraft from awareness of being acquired by a ground-based air-defence battery. The effects would thus be nearly instantaneous, limited in scope to the targeted aircraft, and tactical in nature.

A presence-based attack against the F-35 could take months to prepare, culminating in an elaborate effects phase saved for evoking strategic surprise or for a dire need. Rather than targeting a single aircraft or sortie, attackers would instead target the peripheral networks that interface with the F-35 during its operational life cycle. These could be on-base networks, maintenance forces, or third-party software providers. By doing so, an adversary may temporarily degrade or otherwise completely disable a large number of aircraft.

One supposed innovation in the F-35's software is the Autonomic Logistic Information System, or ALIS. With one ALIS station present at each unit operating F-35s, it allows semi-automated fleet management, mission management, logistics and maintenance[358]. As with other parts of the Joint Strike Fighter program, ALIS has been plagued with critical faults. These faults do well to instruct on two relevant aspects; how ALIS might be vulnerable to presence-based operations, and how exploiting these vulnerabilities could lead to a strategic advantage when triggered in the effects phase.

The issues in ALIS are varied. Attempts to deploy it in test environments forced support personnel to lower network security settings to allow users to log on[359]. Incorrectly handled maintenance data resulted in one instance in "…major damage to a weapons bay door… [360]" from an incorrectly loaded

---

[354] Myron Hura et al., "Tactical Data Links," in *Interoperability: A Continuing Challenge* (Chapter 9 - Tactical Data Links: RAND, 2000), 107–21.

[355] U.S. Department of Defense, "Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF)," 70.

[356] Currently for the U.S., the F-22 and the F-35.

[357] U.S. Department of Defense, "Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF)," 71.

[358] Lockheed Martin, "Autonomic Logistics Information System (ALIS)."

[359] U.S. Department of Defense, "Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF)," 96.

[360] U.S. Department of Defense, 96.

bomb that got loose and struck the aircraft. In June 2017, a software error in ALIS grounded an entire F-35 unit until the issue was addressed[361]. It would therefore seem that the system can both be a boon to aircraft operators and an attack vector for offensive network operators. A single warfighting platform now presents a diverse, varied attack surface that can potentially be exploited during wartime.

Using the common cyber threat framework is useful to establish the key differences between the two high-level ontological categories. Event-based operations have a far lengthier preparation phase as offensive technology is researched, developed, deployed and integrated to warfighters. Conversely, presence-based operations obviously skew more heavily towards the intelligence-heavy presence phase. In each of the four phases – preparation, engagement, presence, and effect – circumstance and characteristics differ between the categories. But even a relative dearth in empirical evidence does not mean they are inscrutable to outsiders. Analysis of previous operations, industry practices, military doctrine, and vulnerability assessments creates a rich tapestry of possibilities and challenges for military network operations.

[361] Sydney J. Freedberg Jr., "ALIS Glitch Grounds Marine F-35Bs," *Breaking Defense* (blog), June 22, 2017, http://breakingdefense.com/2017/06/breaking-alis-glitch-grounds-marine-f-35bs/.

4. Virtual Victory: Applied Cyber-Strategy

Overview

If developing military offensive cyber capabilities is a challenge, effectively weaving them into operations is a gargantuan undertaking. Across all planes of activity – strategic, operational, and tactical – militaries are now facing the inherent difficulty in accommodating a set of tools that offer unique possibilities while creating fresh issues. Contending with these difficulties is paramount to ensuring success, and failure to do so could result in a misapplication of force that may reduce operational efficacy and even risk loss of warfighting contingencies which took months or years to create.

As MONOs appear uniquely novel, military forces may struggle at reconciling their use with existing strategies and operational art. Yet the chasm can be crossed; the existing literature on warfare is highly instructive but requires careful identification of where it converges and diverges from offensive network operations. Examining where MONOs interface with conventional warfare is not an insurmountable task and has been attempted before. Conti and Raymond - influential contributors to both military and civilian information security literature – published a 2017 book on bridging the gap between military and cyber operational art[362]. Greathouse conducted a survey of several classical strategists[363], examining in turn how key terms from each may become applicable to cyber warfare. Numerous other examples abound.

This chapter contends *that presence-based and event-based operations exhibit different strategic principles*. Each sphere has different operational parameters, is often carried out by separate types of practitioners, and results in varying fires and effects. By analysing them as such, contributions by classic strategists and commentators on operational art ranging from Clausewitz to Fuller become eminently more useful to modern intangible warfare. Application of principles such as indirect warfare and battlefield fog of war have natural extensions into cyberspace that should not be discounted by those seeking to operate militarily within it.

Furthermore, an argument will be made that *presence-based operations naturally lend themselves to the strategic-operational planes, while event-based operations are more suitable when viewed as adhering to the operational-tactical planes* (see figure 1). This differentiation can profoundly impact the expectation of results from network attacks, as more localised effects are likely from operational and tactical offenses. Simultaneously, this distinction supports the difficult process of identifying which offensive capabilities should be relegated to battlefield commanders and which should remain within the remit of intelligence agencies or other rear-active forces. While presence-based attacks can

[362] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*.

[363] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," in *Cyberspace and International Relations*, ed. Jan-Frederik Kremer and Benedikt Müller (Berlin, Heidelberg: Springer Berlin Heidelberg, 2014), 21–40.

have grand-strategy significance[364], these introduce a host of legal, political and normative considerations that are outside the scope of this work but should certainly be considered.

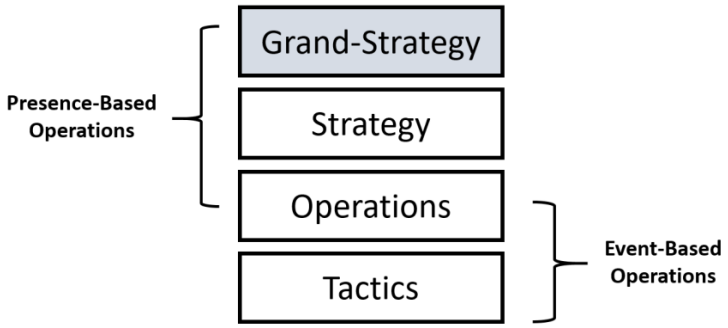

FIGURE 1 - DIVISON OF NETWORK OPERATIONS TO MILITARY SPHERES

The previous chapter addressed the question of *who* carries out MONOs. This chapter builds on that by answering the remaining questions needed to flesh out such use. First, the *why* will be answered by examining the historic contribution of technology to the character and conduct of war. As war historian Michael Howard once claimed, "…whatever changes brought about by social and technological transformation, the essence of 'war' remains.[365]" What follows is an examination of *when* and *where* force should be applied to networks in order to do so most effectively and in harmony with other capabilities. Finally, *what* these operations may actually look like and *how* they are carried out will round out the analysis.

It is natural to try and assess offensive network capabilities with existing strategies. As Arquilla and Ronfeldt pithily wrote, "People try to fit the new technology into established ways of doing things[366]." Analogies employed by strategists and historians equating elements of cyber-warfare to electronic warfare, strategic air power, or even Cold-War era nuclear standoffs are useful. Some of these analogies have been carried out within this work as part of the conceptual framework. But as shown in previous chapters, these analogies do not produce a holistic grasp of what role offensive network operations holds in military thought. The threads binding historical and strategic analysis must be more tightly woven.

While analogies between cyber and kinetic warfare often leave a lot to be desired, integrative conventional strategy is fundamental to success. Simply put, without interleaving MONOs into conventional strategy and doctrine, they may be used incorrectly, or at best used sub-optimally. In order to assure that attacking networks is properly integrated, we must first recognise that elements of existing strategy already incorporate the prerequisite building blocks. In some cases, historic strategists commented on warfare in a fashion inherently hostile to the basic characteristics of cyber

[364] These could include attacks against financial infrastructure, crippling global or regional internet access, or destructive attacks against non-combatant civilian critical infrastructure.

[365] Michael Howard, "How Much Can Technology Change Warfare?," in *Two Historians in Technology and War* (Carlisle Barracks, PA: US Army War College, 1994), 1.

[366] Arquilla and Ronfeldt, "Cyberwar Is Coming!," 41.

operations. In other cases, history represents a powerful foundation upon which modern network strategy can construct.

There are other valuable taxonomies for offensive network activities. Buchanan has similarly identified two different primary types of operations. The first category is similar to presence-based operations, as it includes time-consuming highly-targeted network intrusions initially similar to intelligence operations[367]. The second category offered by Buchanan is markedly different to include indiscriminate wide-scale operations that are not necessarily targeted beyond their original point of entry[368]. These cascading operations often begin with a single point of infection and continue to spread and infect additional endpoints within the targets, causing widespread damage. The first difficulty in this taxonomy is that it excludes most event-based operations viable in a military context, such as attacking specific warfighting platforms with a reusable but ultimately tailored capability. The second difficulty is that while less discriminating offensive capabilities are both easier to develop and likely to exist, they immeasurably raise the odds of incurring collateral damage, an often-dangerous proposition for any but the most total of conflicts.

Healey and Rattray – both prominent contributors to the existing literature on military network operations – offered a more elaborate set of criteria towards categorising such offensives. Healey and Rattray acknowledge the strategic-tactical divide by stating that attacks "…could be in support of existing operations and used in conjunction with other capabilities…" while also "…be used as part of standalone engagements, operations and entire cyber campaign[369]." However, subsequent explanations on their categorisation of cyber-attacks includes six mission types and twelve category parameters, making the distinction somewhat unwieldy as a doctrine-oriented taxonomy[370].

In his 2009 RAND-published research titled Cyberdeterrence and Cyberwar, Martin Libicki offers a distinction between strategic cyberwar and operational cyberwar. The allusion to the strategic and operational spheres may sound similar to the model offered within this thesis, but the intention is quite distinct. Libicki contrasts his typology by indicating that strategic cyberwar is often independent, but most importantly waged in the service of a wider political strategy[371]. Operational cyberwar is thus all network-warfare capabilities as applied against military or military-related targets[372].

Not all theorists uniformly agree that cyber-warfare is a discipline of consequence. In an impassioned call against the supposedly overzealous attention to MONOs, Libicki claimed that the very risk around network security is transient. As he claimed, cyber-warfare can only exist as long as human developers continue to introduce vulnerabilities into code[373]. As methods improve, these vulnerabilities are likely to decrease in quantity and significance, and with it so will the prevalence of

[367] Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*, 78–81.
[368] Buchanan, 81–82.
[369] Rattray and Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," 77.
[370] Rattray and Healey, 81–84.
[371] Libicki, *Cyberdeterrence and Cyberwar*, 117.
[372] Libicki, 139.
[373] Martin C. Libicki, "Why Cyber Will Not and Should Not HAve Its Grand Strategist" (AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST, 2014), 31, http://www.dtic.mil/docs/citations/ADA602106.

offensive network operations for strategic gain. More cautious voices such as that of strategist and historian Lawrence Freedman viewed cyber-warfare as an instrument of potential operational significance, if not strategic[374]. Considering that cyber-warfare has yet to prove its lethality, doubting its strategic contribution is understandable. Instead, by invoking well-known strategic elements, forward-thinking analysts can identify areas in which offensive network operations can meaningfully contribute in a multitude of ways.

WHY - TECHNOLOGY AND WARFARE

What are the key motivations in integrating offensive network capabilities into military operations? Examining history shows several possible explanations, some more compelling than others. Two key themes in particular are worth examining. The first is the relatively modern adoption of technology-first-doctrine-later as the solution to the challenges of warfare. The second is the fundamental human desire to coerce an adversary without shedding blood or undertaking any significant material risk.

Western countries – and first among them the United States – have become increasingly enamoured with the promise of technology since the dawn of the 20th century. As former US National Security Advisor McMaster lamented in 2009, the United States had adopted "an obsession with technology as a defining element of warfare."[375] This premise yielded results against inferior conventional military forces such as Saddam Hussein's Iraqi military in both Gulf Wars. Where technology failed to deliver on its strategic promise was against asymmetric adversaries such as insurgencies. The desire to solve complex military challenges with technology at the expense of the human element proved detrimental to modern US military campaigns[376]. The approach is not inherently a 21st century issue. Already at the height of the cold war strategist Edward Luttwak commented on what he perceived to be an American obsession with acquiring weapons platforms instead of investing in needed strategy development[377].

The advent of precision-based weaponry, network-centric warfare and large-scale joint operations resulted in a widely adopted "capabilities-based" approach to warfare[378]. The belief behind the so-called US revolution in military affairs (RMA) of the 1990s was that technology would usher "dominant battlespace knowledge" and the disproportionate effectiveness of smaller combat forces[379]. A vision of asymmetry-shattering offensive cyber-attacks appealed also to Chinese military thinkers, which in the 2013 issuance of the core doctrinal document Science of Military Strategy mused on how

[374] Lawrence Freedman, *Strategy: A History*, 1. iss. as an Oxford Univ. Press paperback (Oxford: Oxford Univ. Press, 2015), 228–29.
[375] H. R. McMaster, "The Human Element: When Gadgetry Becomes Strategy," *World Affairs* 171, no. 3 (2009): 35.
[376] McMaster, 38–40.
[377] Freedman, *Strategy*, 201.
[378] H.R. McMaster, "On War: Lessons to Be Learned," *Survival* 50, no. 1 (March 2008): 19.
[379] McMaster, 20–23.

targeting critical networks could assist in preventing escalation and unnecessary loss of life when conducting network operations[380].

Prior to the dawn of intangible warfare, strategists had already recognised that technology can upset an existing balance between adversaries. As increasingly effective firearms altered the course of warfare, Clausewitz noted that "violence arms itself with the inventions of art and science in order to contend against violence[381]". Revolutions in logistics as a direct result of railway technology led to far more effective mobilisation of a nation's military force, enabling a totality of war that was previously deemed impractical[382]. Further improvements led to the crippling attrition of the First World War, which was in turn supplanted by the advent of manoeuvre-enabling technologies such as the combustion engine, radio communication, and the airplane[383]. The Second World War unravelled differently to its predecessor, in part as a result of modern technologies being widely adopted and integrated into doctrine.

A comparison between the early days of air power and offensive cyber is meaningful. Both periods initially suffered from the same fundamental flaw; an immense potential was identified but practical uses remained vaguely contoured[384]. Gaps in understanding the nature of the toolset and its utility for warfare meant that hyperbolic scenarios were drawn, and resource investment was disproportionately encouraged towards exciting but untested possibilities. Reflecting the overzealous predictions, perhaps the greatest "silver bullet" analogy between offensive cyber and air power can be found in strategic air bombing.

After the First World War air power strategist Douhet predicted that strategic aerial bombings could physically and psychologically shatter an enemy's national fortitude, thereby eliciting swift capitulation[385]. Engrossed in the possibilities of an unpreventable assault, he proclaimed that command of the air would render other domains of warfare obsolete and that dominance in the domain meant assured victory[386]. Perhaps overly optimistic, Douhet declared it meant being "…in a position to wield offensive power so great it defies human imagination" [387]. However, as historians such as Michael Howard acknowledged, while air power as a component of joint operations has greatly impacted the conduct of war, it had not changed the fundamental truths of it.

Strategic bombing has not historically proven successful at single-handedly compelling victory. As Rattray explained; "…bombing campaigns against cities and general economic targets simply did not cause morale to crumble despite the vast resources invested, casualties inflicted, and damage wrought[388]." The marshalling of the human spirit in light of repeated targeting of civilian

---

[380] McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," 5.
[381] Clausewitz, *On War*, 1:5.
[382] Howard, "How Much Can Technology Change Warfare?," 2.
[383] Howard, 3.
[384] Freedman, *Strategy*, 124; Giulio Douhet, *The Command of the Air*, USAF Warrior Studies (Washington, D.C: Office of Air Force History, 1983), 3.
[385] Douhet, *The Command of the Air*, 23.
[386] Douhet, 27–28.
[387] Douhet, 23.
[388] Rattray, *Strategic Warfare in Cyberspace*, 83.

infrastructure and life resulted in an unyielding stoicism in face of adversity. If anything, examination of conflict may suggest that targeting civilians may solidify homefront unity, as an existential crisis promotes more stalwart civilian commitment to war.

A combination of the persistent lethality consideration and historic evidence on strategic attacks supports the notion that political coercion should not be the primary goal for network operations. Even as cyber was barely considered as militarily viable at the time, Denning already noted in 1999 that "there is no evidence to support the notion that a country's infrastructure could be so disabled by hacking that a government would surrender to a foreign power or alter its policies[389]." That is not to say that limited coercion is never possible by such means; Nye does not altogether dismiss the coercive value of network operations, supporting the idea that they may indeed lead actors to locally alter their course of action[390]. For air power, it took many decades to realise several harsh realities on its strategic limitations, with some arguing that military thought has thus far failed to internalise the lessons of air power[391]. It would therefore be prudent to heed the lessons of history and steer offensive network operations towards more practical goals.

Strategic coercion through the application of intangible warfare is immensely difficult to orchestrate. Most fundamentally, as of 2018 no casualties have been recorded as a direct result of network attacks, so coercion by way of civilian attrition seems unlikely[392]. Additionally, generating collective sustainable impact against elements of national critical infrastructure is no small undertaking. The notion of a national electrical grid that could reasonably be disabled by eliminating a single focal point is in reality rather remote. Infrastructure is most commonly built piecemeal, over the span of decades, and layered with redundancies and fail-safes. When a Russian presence-based operation de-energized elements of the Ukrainian power grid in 2016 and 2017, the effect was limited and remediation took mere hours[393]. It is therefore difficult to generate persistent lethality – against equipment or persons - on a sufficient scale as to achieve significant coercion.

At the same time, the opportunity to coerce with means beyond the physical is becoming increasingly attractive. In 1999, two Chinese colonels internally published a seminal book titled "Unrestricted Warfare". While they are not considered authoritative sources, the book reflected at the time the jarring effects of the perceived American "Revolution in Military Affairs"; the coordinated war machine of the new era seemed world-changing[394]. Liang and Xiangsui's philosophy suggested "…using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interest[395]." Strategic coercion was therefore to be accomplished by employing network warfare as a complementary yet significant component in a larger joint strategy.

---

[389] Denning, *Information Warfare and Security*, 65.
[390] Nye, "Cyber Power," 7–8.
[391] McMaster, "On War," 25.
[392] Libicki, *Cyberdeterrence and Cyberwar*, 122.
[393] Lee, "Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered."
[394] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (PLA Literature and Arts Publishing House Arts, 1999), 4.
[395] Liang and Xiangsui, 7.

When and Where – Applying Force to Networks

Choosing the time and the place for a network attack extends beyond a simple targeting cycle. Should force be applied against deployed forces or command structure? When should sensitive, brittle presence-based assets be activated? What are the guidelines for pacing the use of recurring event-based capabilities in a tactical scenario? These questions can adversely impact operational success. Misapplying force when it is neither necessary or useful may mean permanently losing a capability that could otherwise incur significant costs to an enemy. As before, these are not uniquely cyber-related issues. Strategists have long concerned themselves with several relevant aspects including intelligent use of capabilities via the economy of force principle, as well as examining how force asymmetry and geography matter. Finally, classic terminology such as Clausewitz's centres of gravity will also be examined in relation to MONOs.

Commanders and strategists should aim to maximise the *economy of force*, a key element of modern joint operations. At the heart of the principle resides the understanding that available resources are limited and must be applied intelligently in order to achieve victory[396]. Seemingly trivial to understand but difficult to implement at scale, efficiency is at the heart of all good strategies[397]. Expending overwhelming resources where they are unnecessary means that they may not be subsequently available where the odds are less favourable. Similarly, it is the economy of force that had historically allowed numerically disadvantaged forces to prevail against unfavourable circumstances[398]. By judiciously employing available assets, even asymmetrically weaker adversaries can achieve objectives. Twentieth century strategist Fuller – well known for his unyielding pragmatism - succinctly defined the principle by commenting; "if two opponents face each other, and each possesses an identical supply of force, the one who can make his force persist the longest must win[399]." In so Fuller aptly reflected the practicalities of determining how to strategically employ capabilities. Their usefulness is intrinsically tied to their contextual use.

Some MONOs are difficult to intuitively reconcile with an economy of force. As previously discussed, presence-based capabilities often inflict limited visible effects, require immense prepositioning, and are immediately expended upon first use. Consequently, network capabilities almost seem orthogonal to a commander seeking reliable resources that would be made available when required. Aircraft is reusable after refuelling; stand-off missile stores can be steadily

[396] U.S. Joint Chiefs of Staff, "Joint Publication 3-0: Operations," August 11, 2011, 126.
[397] Liddell Hart, *Strategy*, 323.
[398] J.F.C. Fuller, *The Foundations of the Science of War* (Hutchinson & Company, 1926), 204.
[399] Fuller, 202.

replenished; special forces detachments are flexible and redeployable[400]; these circumstance seemingly do not align with the characteristics of cyber-warfare.

This perception is somewhat misleading. The economy of cyber-force is occluded by looking at it as a single mass of possibilities; event and presence-based capabilities have different considerations for the economy of their use. Researchers have previously alluded to the alternate considerations of network capabilities, indicating for example that due to their sensitivity, commanders are encouraged to first expend their least valuable capabilities first[401]. If force itself manifests differently in intangible warfare, it stands to reason that the economic distribution of force would similarly display in other ways. Presence-based operations can offer either sustained, low-yield deceptive force, or a single burst of visible strategic effect. Event-based attacks – similar to their kinetic counterparts – may offer recurring, gradually diminishing employments of force when deployed intelligently alongside other capabilities. Economic use can still be attained, but the considerations for achieving it are different between the two categories.

Presence-based operations indeed do not conform to conventional perceptions of economy of force. With non-negligible odds of failure, they lack the visceral reliability of many kinetic capabilities. Premature detection of offensive intent prior to the effects phase could result in a complete loss of operational capability[402]. However, successfully activating an effect at an opportune moment can result in a high-yield effect that could alter the entire operational calculus. As such, presence-based capabilities should not be ignored; they simply must be properly accounted for[403]. Indeed, as previously suggested, the economic consideration is vastly different if deploying presence-based capabilities stealthily or overtly.

A stealthy deployment of presence-based capabilities means a diffusion of the effect. A promising albeit non-military case study demonstrating a stealthy gradual effect is the Stuxnet malware deployed against the Iranian nuclear project. Rather than creating a single destructive effect against the centrifuge cascades within the Natanz facility, the malware deceptively influenced both software and hardware over an undisclosed but lengthy period of time[404]. The strategic effect was achieved by maintaining the presence phase over an extended timescale, dispensing an effect in a controlled, diffused fashion. It is a useful example of how operations can represent a highly economic use of limited force; comparable military scenarios could have significant utility.

Alternatively, an overt effects phase for a presence-based operation can result in a single-shot, high-yield effect. Expending such a capability may represent the culmination of years of operational effort to pursue a single operational or strategic objective. One such plausible scenario would be a

---

[400] This is in part the reason special forces are viewed as favourable enablers of the economy of force. They require minimal preparation, are dynamic and flexible assets, and can assist conventional forces by reducing the danger to them. See U.S. Joint Chiefs of Staff, "Joint Publication 3-0: Operations," 126.

[401] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 204.

[402] See analysis of the operational effects phase in the previous chapter.

[403] The volatile value and sensitivity of presence-based operations is reflected by the level of approvals they often require. See for example U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities," 38.

[404] Langner, "Stuxnet - Dissecting a Cyberwarfare Weapon."

wide-scale sudden disruption of military satellites servicing an operational theatre. Such an attack could impair navigation, targeting, and intelligence efforts, all crucial in combat operations. However, activating such a capability would nearly ensure its detection, thereby allowing defenders to eventually expunge the malicious presence out of their networks. Such an attack would therefore best be employed alongside a massive kinetic effort, preferably one that capitalises on the new weakness exposed as a result of the offensive.

Maritime vessel collisions highlighted the fallibility of navy assets. In 2017 alone, several incidents involving US Navy destroyers resulted in severe damage and casualties. Issuing an investigation report, the Navy concluded that a series of human error and sub-par operating procedures resulted in the crashes[405]. Simply put, onboard staff failed to correctly operate systems according to established procedures. While this does not immediately indicate that network or software vulnerabilities are present, it alludes that tampering with shipboard systems may well go unnoticed, with human verification methods insufficient to prevent even catastrophic collisions with unrelated civilian vessels. Were a capability to tamper with shipboard telemetry and navigation exist, engaging it in the early phases of combat could result in a significant operational gain.

An event-based capability should be able to repeatedly dispense its payload against different targets. For example, a protocol denial of service MONO targeting tactical communication networks by flooding them with superfluous control messages could degrade the operational capacity of local units[406]. While such a capability is inherently more robust and reusable, diminishing returns are expected as local forces eventually realign, adopt evasive procedures and attempt to mitigate the attack in various ways. Thus, while repeat uses are available, judicious dispensing of the capability is advised as to avoid the eventual inoculation by defending forces.

The most straightforward answer to "where should force be applied to networks" is "where it counts". While this might appear trivial, doing so effectively is subtly difficult. As previously discussed[407], identifying and prioritising virtual targets can be a laborious affair requiring high-quality intelligence and intimate familiarity with the adversary. While networks and digital links may seem more abstract than their physical counterparts, the intelligent application of force to adversary weak points is not new. Much like other military principles, effective targeting that will result in substantive impact has long since been the desire of tacticians and strategists alike. One of the oldest yet most renowned conceptualisations of this desire is Clausewitz's centres of gravity.

A centre of gravity is merely where military forces are concentrated *en masse* so that a successful strike against would result in an effect permeating all enemy warfighting efforts[408]. Adopted by many subsequent strategists, each had either built upon the original definition or altered it to suit their

[405] U.S. Navy, "Report on Collisions Involving USS John McCain and USS Fitzgerald" (Office of the Chief of Naval Operations, October 23, 2017).
[406] Study of the targeted protocol would be necessary to effectively spoof its control messages
[407] See the "preparation" phase of the previous chapter, where targeting was covered at length.
[408] Clausewitz, *On War*, 1:317.

messaging[409]. As various balance-upsetting technologies emerged, theorists were inclined to believe that it could be used to directly strike at enemy centres of gravity, bypassing forces set to defend them and directly dealing a crushing blow.

Intangible warfare gradually led to the emergence of new centres of gravity[410]. As modern military forces became reliant on continuous data feeds, situational awareness, and instantaneous communication, striking the operational core of these became an operational objective. While agility may allow well-trained forces to recover relatively quickly, within the course of an engagement blinding or confusing an enemy could now prove crucial. If the modern joint operations military is an organism, the command core is its heart and communication networks its arteries. A successful attack against the core could result in systemic failure across the entire organism. At the same time, analysis must be cautious not to misappropriate the significance of mass in Clausewitz's centres of gravity. When Conti and Raymond listed their own "cyber centres gravity" – they included supply chains and telecom infrastructure[411]. While logistics and infrastructure represent high-value targets, they are not per se a concentration of mass.

Centres of gravity are often conflated with Jomini's decisive points. Where the former concept represents the concentration of warfighting mass, the latter relates to any location or target which – if attacked – would result in substantial effects[412]. Centres of gravity are often not directly targeted in warfare, as they are by definition hard targets and challenging to overwhelm, thus representing an unfavourable choice for direct attack[413]. Instead, decisive points could be logistics, communications, or border zones for which an attack could adversely affect the centre of gravity. Rather uniquely, cyber-warfare changes that calculus; centres of gravity and decisive points now frequently overlap and are attractive targets. New networked centres of gravity have now become viable decisive points, as a limited application of network force could result in highly substantive effects without committing to an unfavourable direct military clash.

Targeting an enemy's information centre of gravity with an offensive network operation could theoretically permit bypassing its fielded military forces altogether[414] – at least initially. While Clausewitz initially considered such centres as mere amassments of enemy force, they can be viewed through a modern prism as targets which – if attacked – would cause a cascading effect extending well beyond the target. Attacking an informational centre of gravity can disrupt lines of communication and control and increase the debilitating significance of what Clausewitz called the "fog of war"[415].

Opposing forces are rarely at parity; asymmetry is nearly always assured. Even in a seemingly bi-polar circumstance such as the Cold War, the United States and the Soviet Union were never equal in their capabilities. Soviet technology proved immensely capable at ballistic missile technology, while

[409] See for example Jomini, Liddell-Hart, and Fuller, all three of which discussed similar or overlapping concepts.
[410] Rattray, *Strategic Warfare in Cyberspace*, 27.
[411] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 187.
[412] Schneider and Izzo, "Clausewitz's Elusive Center of Gravity," 51–52.
[413] Liddell Hart, *Strategy*, 145–46.
[414] Rattray, *Strategic Warfare in Cyberspace*, 182.
[415] Greathouse, "Cyber War and Strategic Thought," 30.

the United States was unparalleled in its adoption of computerisation. Adversarial asymmetry is fundamental to warfare both historically and in modern circumstances, and can manifest equally both in materiel, troop quantities and even will[416]. However – and as history instructs – conventional overall weakness does not necessarily mean defeat. Even staunch proponents of numerical superiority such as Clausewitz recognised that overall numbers may not be necessary. It is the ability to bring superior numbers to decisive engagements in conflict that epitomizes an effective strategy[417]. Other strategists recognised that numbers may not be necessary at all, as long as the capacity of the enemy to employ them is degraded.

Strategists have focused heavily on nullifying adversary advantages and through that minimising asymmetries. What is strong could be made weak, perhaps even prior to conflict. As Sun Tzu put it; "Though the enemy may be stronger in numbers, we may prevent him from fighting[418]." When Chinese officers reviewed the performance of American war efforts in the first Gulf War, they reacted with alarm to the gaping chasm that has opened between the US forces and all their would-be adversaries[419]. The only way to contest such a force would be through the adoption of innovative capabilities that would negate American network-centre warfare, thus reducing the effective ability of US forces to bring their forces to bear. Insurgencies such as in Afghanistan or Iraq and sub-state entities such as the Palestinian Hamas have tacitly embraced such an approach as a core tenet of conflict: In the absence of conventional might – innovate.

Cyber-warfare draws heavily on asymmetries. Where there is parity between adversaries, cyber-warfare can occasionally be used to tip the balance. Offensive network operations can be used by a conventionally weaker adversary to reduce technology-centric power discrepancies. They could also be used by an asymmetrically potent force to capitalise on technological superiority to shatter already weaker network defences. It could even be used to generate false asymmetries, by altering adversary perceptions of available forces. Quite simply and in contrary to some conventional wisdom, cyber-warfare is not necessarily the toolset of the weak. It is simply a versatile toolset.

One possible use for presence-based operations is by insurgents. Conventionally disadvantaged, insurgencies often rely on creative application of force to create disproportional effects against a stronger adversary. Instead of tangling directly with massed forces, gradually bleeding the enemy can eventually result in unacceptable costs. However, in order to do so, insurgent forces must successfully degrade or subvert technological advances held by the stronger party. Offensive network operations offer an interesting opportunity to do so. Perhaps this has yet to happen as most modern insurgencies have occurred in countries traditionally bereft of significant internet penetration. A lack of familiarity and expertise means that targeting valuable networks becomes unfeasible. Yet, circumstance would

[416] Edward A. Smith, "Effects Based Operations," *Applying Network Centric Warfare in Peace*, 2005, 43.
[417] Clausewitz, *On War*, 1:164.
[418] Sun Tzu, *The Art of War*, 2004th ed. (Sheba Blake, n.d.), 57.
[419] Liang and Xiangsui, *Unrestricted Warfare*, 100.

differ were an insurgency to occur within a more technologically capable nation. This is not a purely theoretical scenario; the spectre of conflict against nations such as Estonia and Iran is not unrealistic.

In 2014, 25-year-old British man Sean Caffrey successfully compromised a US Department of Defense satellite network used to communicate with global partners and personnel[420]. The Enhanced Mobile Satellite Services (EMSS) allowed dispersed assets to securely communicate using commercial infrastructure. At the time, Caffrey satiated his curiosity by publicly releasing a list of 30,000 phone numbers and the details of 800 network users. Were such a compromise to have taken place by a hostile threat actor – the result could range from assisting in gathering targeting intelligence on local personnel to compromising details on planned operations. In times of conflict, the network and its neighbours could have found themselves targeted by a MONO seeking to disable or influence them. It clearly did not require significant expertise or dedicated resources in order to successfully target the military network.

Networks may transcend geography but they ultimately remain subordinate to it. While information is carried globally at tremendous speed and volume, traffic facilitated by a physical infrastructure[421]. Impair the infrastructure, and the virtual component would be similarly impaired. Thus, while the US and its NATO allies have deemed cyberspace as an independent domain of warfare, it is in fact the penultimate one which permeates through all others. Land, sea, air and space all facilitates the transit of networks, and consequently one can attack the latter through one of the former. US doctrinal documents themselves acknowledge this approach, with diagrams of the modern operational environment visualising cyberspace as interwoven into all physical domains[422].

It is difficult to wholly sever most nations' connection to the global internet. Difficult, but not altogether impossible[423]. In many cases, nations rely on several high-volume fibre-optic cables to carry the bulk of their internet traffic beyond their borders. Consequently, severing these crucial data arteries could effectively cripple a nation's access to the internet, as providers would be forced to fall back to limited-bandwidth, high-cost solutions such as satellite connections. One such notable incident occurred in 2008, in which two distant undersea cables carrying much of the Middle East's internet traffic were severed, supposedly by a combination of inclement weather and wayward ship anchors[424]. The result was staggering; Egypt reportedly lost 70 percent of its internet traffic, while other nations similarly suffered. A decade later, United States officials reported with alarm increased activity by Russian submarines as they prowl known undersea cable routes[425]. The risk to internet infrastructure remains substantial.

---

[420] David Bisson, "Hacker Admits to Stealing Military Data from U.S. Department of Defense," *Tripwire*, June 16, 2017, https://www.tripwire.com/state-of-security/latest-security-news/hacker-admits-to-stealing-military-data-from-u-s-department-of-defense/.

[421] Nye, "Cyber Power," 9.

[422] U.S. Joint Chiefs of Staff, "Joint Publication 5-0: Joint Planning," 114.

[423] Some nations have more international communication links to the global internet than others.

[424] John Borland, "Analyzing the Internet Collapse," MIT Technology Review, accessed January 27, 2018, https://www.technologyreview.com/s/409491/analyzing-the-internet-collapse/.

[425] David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times*, October 25, 2015, sec. Europe, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

The geographic aspect of network warfare creates new complications. Beyond the general risk of collateral effect, attacks against networks risk unintended damage against third parties. This is a plausible prospect; militaries often rely on civilian telecommunications infrastructure. Public global infrastructure used for military purposes is often shared by multiple other countries for civilian use[426]. Attacking infrastructure or even information conduits such as local satellites or optical fibre trunks can cause significant damage that extends far beyond the parties at conflict.

Intentionally co-opting third parties is also a significant risk. Stationing military equipment on foreign soil is both highly visible and nearly impossible to carry out at scale without overt permission from the hosting country. Conversely, offensive cyber capabilities could easily use third-party servers without the knowledge of these nations. It raises key issues of complicity when one party to a conflict is attacked through an unwitting intermediate[427]. It can be challenging for a victim to assess the willing co-operation of the intermediate, or even the degree of control that the attacker has over the third-party assets[428]. There is therefore a substantial risk of drawing additional participants into conflict, thereby intentionally or unintentionally increasing the scale of war.

A small preview of the dangers of network geography can be seen in the 2008 Russo-Georgian War. The conflict offers a rudimentary example of offensive network operations due to the then-nascence of Russian doctrine and the technological limitations of the Georgian network infrastructure[429]. Yet, one incident stands out. After a denial of service attack knocked out Georgian government websites, they were relocated to civilian US jurisdiction to avoid follow-up attacks. The websites however were not hosted by the US government, but rather by a small privately-held company named Tulip Systems[430]. By any kinetic equivalent, this could potentially then expose the company, its assets, and peripheral providers to attack by both the Russian government and its supposedly unaffiliated hacktivist supporters. Were subsequent attacks to occur with damage incurred to US infrastructure, it could indeed evoke undesired consequences.

What and How – Manoeuvres

Absent physical assets, manoeuvring manifests different in network warfare. As the US officially defines it, a manoeuvre entails moving materiel and personnel to an advantageous position in respect to the adversary. This may or may not be in tandem with an actual effect[431]. Networks sidestep many physical constraints, but all notion of manoeuvring is not inherently rendered obsolete. Examining

[426] This is especially true considering the rise of "cloud computing", distributed networks that dynamically allocate resources to users. Amazon is one of the globally largest providers of such services, including the U.S. government. On this risk, see for example David Midson, "Geography, Territory and Sovereignty in Cyber Warfare," in *New Technologies and the Law of Armed Conflict*, ed. Hitoshi Nasu and Robert McLaughlin (The Hague: T.M.C. Asser Press, 2014), 78.

[427] Ashley Deeks, "The Geography of Cyber Conflict: Through a Glass Darkly," 2013, 5.

[428] Deeks, 13–14.

[429] The gradual development of Russian offensive network operations is assessed at length in the dedicated subsequent chapter.

[430] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (2008): 66–67.

[431] U.S. Joint Chiefs of Staff, "Joint Publication 1-02: DoD Dictionary," 149.

how timeless concepts in operational manoeuvring such as surprise, deception, and destruction apply to network warfare reveals an organic fit with historic strategic thought.

Many of the core characteristics of manoeuvring remain uniquely useful to network warfare. By electing to integrate observations on MONOs with classic terminology used to describe kinetic warfare, supporting joint operations and facilitating meaningful battlefield effects becomes more feasible. If senior military leadership can reflect on how surprise, deception, speed, destruction, and centres of gravity translate to network warfare, they will be far better positioned to incorporate such tools into their pursuit of objectives. Understanding how manoeuvres in cyber-warfare differ or not from kinetic warfare can promote their responsible use.

Achieving *surprise* is an ambitious but worthy goal. Liddell-Hart had labelled attaining surprise as one of the most vital elements in war[432], and Clausewitz placed it "at the foundation of all undertakings[433]." It is a quintessentially timeless aspect of warfare, referring to the art of attacking an unsuspecting target at an unexpected time[434]. Tactical surprise entails forcing an adversary into a localised battle under suboptimal conditions to the enemy. Strategic surprise is achieved if the actual state of war has been unexpectedly forced upon an enemy, thereby causing disadvantageous resource allocation, disposition of forces, state of readiness, and overall capacity for defence.

Attaining tactical surprise is commonplace whereas strategic surprise is a far more difficult ruse - yet potentially one of a far more significant payoff[435]. The practicality of strategic surprise has been called into question; how can sizeable troop movements and marshalling for war be performed without alerting the intended victim and triggering an escalatory cycle? Clausewitz himself wondered as much, as he wrote that "In idea [surprise] promises a great deal; in the execution its generation sticks fast by the friction of the whole machine. In tactics the surprise is much more at home… it rarely happens that one state surprises another by a war[436]."

Strategic surprise is not unheard of. In 1973 - still aloof from former victories and discarding numerous warning signs – Israel was simultaneously attacked on multiple fronts by Syrian and Egyptian forces. Despite intelligence to the contrary, massed forces were incorrectly assessed to be participating in large-scale drills. What came to be locally known in Israel as the Yom Kippur War was a resounding strategic surprise, which resulted in massive initial casualties. While the Israeli Defense Forces eventually recovered, memories of the successful ruse remain a painful national scar.

In presence-based operations, surprise may manifest as a prelude to the opening salvo of conflict. To mask large-scale movement of forces or the intent to attack, MONOs may be used to disable or otherwise degrade early warning and situational awareness systems. Alternatively, targeting military equipment may reduce available adversary assets, while targeting infrastructure could sow useful

[432] Liddell Hart, *Strategy*, 34.
[433] Clausewitz, *On War*, 1:168.
[434] Tzu, *The Art of War*, 32.
[435] Clausewitz, *On War*, 1:284.
[436] Clausewitz, 1:169.

chaos. This would then allow attacking kinetic forces to operate with relative impunity, increasing the odds that a gambit at strategic surprise may succeed. As a result of their extensive clandestine pre-positioning, presence-based operations are highly congruent with the strategic principle of surprise.

In event-based operations, surprise may be limited to a tactical play. A MONO against local assets could be used to increase the fog of war, thereby facilitating manoeuvres that would otherwise result in direct engagement with an adversary[TKTK – include reference from class, session 10]. As MONOs do not necessarily generate visible effects, they could even avoid tipping victims off to having been attacked, thereby affording kinetic units to surprise an already-degraded enemy. By targeting networks, it now becomes viable to initiate hostile contact while one party remains unaware.

Clever use of *deception* can help capitalise on advantages or reduce disadvantages. History and strategy are particularly instructive on the value of deception to strategy and operations. Strategic thought on deception includes Sun Tzu's well-known mantra that "all warfare is based on deception[437]", Machiavelli's predilection to pragmatic deceit[438], and Clausewitz's remarks on attempting "…to lead the enemy to make a false conclusion[439]" as a key part of offense. Modern observers have correctly identified deception as particularly potent when applied to cyber-warfare[440], as the potential impact on the trust between man and machine could be highly significant.

Deception in cyber-warfare entails fooling both man and machine by targeting the latter. Barring future advancements in artificial intelligence, deceiving devices may be accomplished by tampering with sensory inputs, thus causing them to predictably to generate false output[441]. A machine inherently has no reason to doubt its trusted pipelines of information unless explicitly instructed to do so and may accept false input as real as long as it is constructed and authorised correctly. Much like deploying inflatable tanks to fool spotters, creating a digital equivalent of an optical or aural illusion can be useful. It is in recurring success where deception becomes difficult. As Libicki noted in his scepticism of its overall utility, if the deceptive component of a network attack is detected it becomes far less likely to be subsequently successful[442]. Much like with malware itself, detection of deception means inoculation. Where deployed tank dummies may continuously foil adversary reconnaissance efforts until sensory technology is improved, network deception is far more difficult to maintain.

The tenuous recurring value of deception is not unique to intangible warfare. As Freedman notes, even as the ancient Greeks introduced strategists to "cunning" as an element of war, they similarly revealed that an overreliance on deception would offer diminishing returns[443]. As an adversary became gradually more aware of being manipulated, deception itself as an operational effect would

[437] Tzu, *The Art of War*, 31.
[438] Freedman, *Strategy*, 51.
[439] Clausewitz, *On War*, 1:217.
[440] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 242.
[441] Conti and Raymond, 34.
[442] Libicki, "Why Cyber Will Not and Should Not HAve Its Grand Strategist," 34.
[443] Freedman, *Strategy*, 23.

become less impactful. Much like other characteristics of network warfare this is still true today, if exasperated greatly. Deception on its own will not result in victory[444].

Classic strategy as envisioned by Clausewitz enshrines the destruction of enemy forces as the only meaningful way of attaining strategic victory. All other pursuits in war are peripheral to the practice of taking lives and destroying materiel[445]. This notion may at first seem intrinsically hostile to network operations, where offensives may impair systems but rarely exact a physical cost. But even Clausewitz – a rather extreme figure in his adherence for force destruction – acknowledged that impairing the capacity and collective will to fight is similarly crucial to success, as "…nothing obliges us to confine this idea [of destruction] to the mere physical force; … the moral is necessarily implied as well[446]."

Whether destruction is a mandated part of all offensive capabilities is up to debate. While Clausewitz was famously focused on activities eventually coalescing around adversary force destruction, some historians such as Delbruck delineated well between a strategy of annihilation and a strategy of exhaustion[447]. Others such as British strategist Corbett recognised that even in Clausewitz's writings, strategy did not singularly need to focus on decisive battlefield victories by way of destructive force[448].

Network attacks offer an interesting dichotomy of destruction; they are simultaneously capable of immense collateral damage and unprecedented pinpoint accuracy. Both considerations are worth separately unpacking, as they both must be considered when choosing to employ MONOs against a target. Applied correctly, modern intangible warfare can be the "ultimate precision weapon", as labelled by Rattray[449]. Indeed, the gradual increase in precision targeting is a fulfilment of the underlying premise of technology-assisted warfare[450]; cyber is merely the continuation of this trend. As the previous chapter detailed, the elaborate targeting cycles of presence-based operations support this notion. Operations include extensive periods of lingering within adversary networks and conducting repeat micro-targeting cycles against specific servers. Offensive payloads must be specifically crafted and configured to work against the target. As a result, the surgical fitting of payload to effect[451] implies peerless specificity and control over the intended impact.

Collateral damage exceeding the intended targets is a nearly unavoidable risk in network warfare[452]. Even a seemingly localised event-based effect can escape its operational boundaries and potentially wreak havoc on a wide scale if improperly developed and constrained[453]. As US doctrine acknowledges, "collateral damage from this type of attack is not always predictable[454]"'. For event-

[444] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 249.
[445] Clausewitz, *On War*, 1:33.
[446] Clausewitz, 1:36.
[447] Freedman, *Strategy*, 108.
[448] Freedman, 118.
[449] Rattray, *Strategic Warfare in Cyberspace*, 21.
[450] McMaster, "The Human Element," 35.
[451] Rattray, *Strategic Warfare in Cyberspace*, 192.
[452] U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities," 40.
[453] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 46.
[454] U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities," 13.

based attacks, a cascading destructive attack against a local network might permeate well beyond it if operators are not cautious. Considering the modern battlefield often relies on dual-use infrastructure shared between military forces and civilian population, the result can be a catastrophic loss of internet access or data that would be difficult to leash once activated. The 2017 NotPetya worm - originally targeting Ukrainian servers and computers – quickly led to a blaze of infections that resulted in digital damage to many thousands of devices worldwide[455]. For presence-based attacks, engaging destructive payload against an identified networked centre of gravity can similarly have unexpected consequences. In one example, an overly-successful attack against military aviation could have ramifications on civilian aviation, as a result of data-sharing conduits or collaborative air traffic monitoring services.

Network attacks are often disregarded as they result in transient effects[456], further compounding their effective use. Weapons seemingly have limited utility have if their effects are primarily ephemeral, making them potentially unreliable. Deconstructing this argument, we are left with three contestable claims; (1) that the effect is disruptive rather than overtly destructive; (2) that damage applied to software is easily recoverable; and (3) that the weapon viability itself is transient. All three are worth deconstructing in turn.

Disruptive attacks may still have immense value, strategic or otherwise. On the campaign scale, a well-positioned presence-based attack can enable strategic surprise, as occluding adversary sensor grids can introduce sufficient delay into an adversary's decision-making cycle can cause an incoming opening salvo to go unnoticed. A failure to scramble defenders due to disrupted intelligence can result in a hefty strategic cost, redistributing relative advantages and potentially knocking out assets that would otherwise come into play. Event-based attacks can similarly be used to create a temporary breakdown in command and control, thereby facilitating kinetic strikes.

Overall damage from network-warfare is indeed often easier to recover from. Physical effects from such attacks are a rarity. Principles of network resilience, which include the use of redundancies, backups, and emergency procedures should in theory reduce the destructive value of software attacks. However, military conflict unfolds at a rapid pace. Once an attack has taken place, recovery would still take precious time, during which the impacted system will be inactive. In some cases, theatre-deployed assets to do not have the means to completely restore their own software. Consider a navy destroyer that suffers from a catastrophic corruption of its shipboard systems. As shipboard-staff are merely operators of weapon platforms developed in the defence industry, special expert staff would be required to restore the ship to functionality. In such cases, this would require a costly trip back to a friendly port, where an extensive repair and readiness cycle would be undertaken to recover ship

[455] Shipping giant Maersk was one such victim, with allegedly 4,000 servers and 45,000 personal computers requiring full reinstallation. See Richard Chirgwin, "IT 'heroes' Saved Maersk from NotPetya with Ten-Day Reinstallation Bliz," *The Register*, January 25, 2018, https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

[456] Rattray and Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," 79.

functionality. By the time the ship is ready to re-enter the conflict, it may have already missed it entirely.

The notion that offensive network capabilities are transitory stems from the idea that detection means inoculation. As previously discussed, this is true in some cases but not all. As Max Smeets notes, well-resourced forces can mitigate the perishability of their offensive capabilities by investing in robust, modular, and difficult to detect platforms[457]. This in turn can be applied to the typology used in this thesis. Event-based capabilities would rely on hard to patch or systemic vulnerabilities that are not easily mitigated. Presence-based operations would attempt to ensure operational security so that capabilities are not wholly compromised when used.

Wars rarely occur on conveniently open battlefields. Where once rows of infantry and cavalry would bear down upon similarly ordered enemy hosts we now see urban warfare, standoff weapons and multi-domain combat theatres. Indeed, this is one of the most pervasive criticisms of Clausewitz's classic tenets on applying maximum force to an adversary's concentration of military power; it seems a distinctly inefficient way of conducting modern warfare. Clausewitz criticised the notion that victory could be attained "…by means of small but extremely well-directed blows to produce such paralysation of the enemy's forces…[458]". But as technology created new asymmetries and the means to effectively manoeuvre around defences, it became less clear cut.

Having more troops to field classically translates to an increased chance of strategic success[459]. However, it was always assumed that numerical superiority cannot always be assured. In some conflicts, especially those forced upon an enemy by a challenger of superior positioning, numerical superiority is simply unattainable. Yet one does not need to always have the numerical advantage; it may be sufficient to possess it at key operational moments within war[460]. Rather than amass numbers, the eventual goal became the "concentration of strength against weakness", as Liddell-Hart aptly described it[461].

Cyber-warfare presents a key opportunity to conduct what Liddell-Hart famously called the *indirect approach*[462]. The concept is seemingly quite basic; avoid direct engagement with an enemy's massed front, instead opting to subvert defences and advantages by locating weak points. Possibilities include attacking under-protected flanks and capitalising on elements such as surprise. These options allow military planners to maximise force projection, prevent unnecessary casualties, and potentially even shorten the duration of conflict[463]. While often lauded for the term's inception, Liddell-Hart certainly did not give birth to the overall strategy of avoiding direct conflict. Sun Tzu already favoured

[457] Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies*, February 16, 2017, 1–28.
[458] Clausewitz, *On War*, 1:205.
[459] Clausewitz, 1:164.
[460] Clausewitz, 1:167.
[461] Liddell Hart, *Strategy*, 334.
[462] Liddell Hart, *Strategy*.
[463] Liddell Hart, 145.

a combination of direct and indirect manoeuvres, as he believed that the combination of both is paramount to ensuring overall victory[464].

Presence-based operations are intrinsically about bypassing defences. The process of clandestinely intruding upon enemy networks and prepositioning assets overtly indicates a desire to silently avoid network defences. The logic for this is quite simple; friction with defensive lines means detection, and detection is the bane of presence-based operations. Thus, such operations are best served to facilitate indirect advantages.

Presence-based operations can also create altogether new flanks[465]. A successful compromise of a command and control centre can create situational blind spots by reducing the enemy's capacity to react or by causing it to falsely redistribute its attention. Similarly, a successful compromise of logistics or maintenance infrastructure may affect the deployment of forces, thereby reducing the capacity of the force to act jointly. Network operations can therefore facilitate a weakening of massed forces, either by degrading the front or opening undefended pockets that could then be targeted for indirect attack by conventional forces. Thus - if integrated correctly - presence-based operations may be the quintessential enabler of Liddell-Hart's indirect approach.

A key element in manoeuvres is *agility*. In warfare, agility commonly pertains to the effectiveness in which a combatant can shift from one circumstance to another; it is a measure of dynamics[466]. Circumstances include both purposeful and unexpected changes between states. The former can occur simply when trying to adapt from one operational scenario to another, while the latter occurs when entities are forced to adapt to a change. Agility is thus a measure of speed, adaptability, and resilience[467].

Agility is heavily addressed in modern warfare doctrine as a prerequisite for conducting effective joint operations[468]. The rise of network-centric warfare emphasising the deep fusion of technology with the decision-making process means that the operational tempo has markedly increased, thereby requiring all participating forces to be increasingly agile to keep up[469]. Concurrent sensory input from dozens of sensors both local and remote can assist in engaging numerous targets in rapid succession or even simultaneously. Forces must be able to respond, redeploy, and in some cases switch payloads to be able to fulfil an entirely different mission package. Agility may also occur on a strategic scale; the sudden need to respond military to an escalating situation may require disparate forces to suddenly and wholly realign priorities.

Agility is particularly fascinating as it is one of the key areas in which event and presence-based operations differ. Agility for event-based operations reflects one of the greatest difficulties in offensive

---

[464] Tzu, *The Art of War*, 47–48.
[465] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 94.
[466] David S. Alberts, "Agility, Focus, and Convergence: The Future of Command and Control" (Office of the Assistant Secretary of Defense for Networks and Information Integration, 2007), 23.
[467] Anthony H. Dekker, "Measuring the Agility of Networked Military Forces," *Journal of Battlefield Technology* 9, no. 1 (2006): 3.
[468] U.S. Joint Chiefs of Staff, "Joint Publication 5-0: Joint Planning."
[469] Smith, "Effects Based Operations," 54–60.

network operations; they have to be robust. No matter the circumstance, whenever an operator "fires" an event-based capability at an adversary, it must work. This is particularly difficult due to the inherent sensitivity of malicious software to minute changes in the adversary environment. If the vulnerability it exploits is no longer present, or if the attacked platform is configured differently than what the attack tool needs in order to function, it may cause an unexpected effect or altogether fail. Thus, even the most specific event-based attack capability has to be agile in order to foster commander trust and be properly integrated into operational planning. An unreliable capability is one that will not be chosen when the need arises.

Presence-based operations initially appear almost antithetical to agility. Requiring extensive pre-positioning, tailor-made attack tools, highly-focused intelligence, and almost no reusability, such capabilities seem intrinsically hostile to a high-paced operational environment, in which "…forces must be prepared to transition rapidly from one type of operation to another[470]". This is indeed one of the key reasons why they are best suited for strategic or theatre-level effects rather than localised operations which experience more variable changes in circumstance.

Albeit differently, agility can still manifest for presence-based operations. Rather than flexibility at the operational level, presence-based agility can manifest as robustness and modularity of the attacking infrastructure itself. Often, high-quality nation-state malware is modular in nature[471], indicating a strategic understanding that a flexible, modular tool could be adapted to specific needs as an operation unfolds. The intrusion and lateral movement mechanisms may stay the same, with attack modules developed and deployed as required for specific target types. By strategically investing in such capabilities, military planners can shorten the time it takes to develop an operational solution against a high-value presence-based target once it is compromised. Agility remains relevant, but relates to an entirely different scale of time.

CONCLUSIONS

Novelty should not prevent utility. Accrued strategic thinking can contribute vastly towards understanding the opportunities and limitations of offensive cyber capabilities if applied in meaningful ways. The challenge resides in embracing the unusual circumstances of operating through and against networks. There is no denying that the lack of a kinetic component forces a substantial change in approach. Centres of gravity are different; the meaning of the manoeuvre thus changes as well. Military strategy can apply to these, it simply applies in other ways.

This chapter is certainly not the first text to suggest that offensive network operations can be utilised across different planes of military thought – the strategic, the operational and the tactical. The meeting of two crucial axes – the event/presence-based approach and the application of historical military thinking – are what make this contribution unique. This chapter did not seek to contradict

[470] U.S. Army Headquarters, "Army Doctrine Publication 3-0: Operations" (U.S. Army Headquarters, October 2011), 2.
[471] Monte, *Network Attacks & Exploitation*, 124–25.

previous findings but rather channel them further in meaningful ways. By further distinguishing between operational types using a helpful taxonomy, two decidedly different operational approaches emerge. Both approaches have their own set of circumstances distinct to them, both can and should be used by distinct operators for diverse purposes.

Presence-based operations are naturally incongruent with a battlefield tempo. Their targeting phase is ponderous, and they require significant prepositioning. Establishing even a single presence-based capability against a hardened target of military value can take many months. However, once established, high-level command staff must be aware of the potential strategic utility of such capabilities. If a deceptive element can be incorporated into the activation phase, its effects could possibly stretch on for the duration of the conflict. Subtle malicious manipulation of command and control telemetry, or minute disturbances in targeting latency could wreak havoc across an entire operational theatre. Conversely, if protracting the engagement is not feasible, a single activation burst could similarly prove lethal in the earlier stages of conflict. Fully blinding satellite communications as a result of a network attack could significantly degrade operational capacity until its restored, possibly even taking days to do so. Such a stretch of time is critical at the onset of combat operations.

Event-based operations can and should be delivered to deployed units. Where offensive cyber cells operate, they should have pre-packaged, resilient tools for their use. Such capabilities could allow them to temporarily degrade tactical communication networks, wipe local adversary networks, or blind vehicle-borne systems used by aircraft, maritime vessels and ground forces. As adversaries become increasingly networked themselves, their cyber-attack surface commensurately grows. It is increasingly becoming possible to weaponise the adversary against itself; one only needs to target the systems that have become its operational crutches.

The infatuation of modern militaries with technology resulted in capability-based strategies rather than strategy-contributing capabilities. Originally a twentieth century phenomenon, the desire to offset adversary advantages by winning technologically is untenable in network operations. Overreliance on air superiority arguably resulted in degradation of capacity to effectively hold territory. Adoption of drones and remote strikes similarly increased the distance between decision makers and the battlefield, resulting in protracted, gainless conflict. We must not repeat mistakes with network capabilities.

Strategic coercion of an adversary will not likely occur as a result of overwhelming its networks. Instead, understanding the centrality of networks to modern life and combat operations means identifying how centres of gravity have now uniquely become targetable. Where forces shunned concentrations of military mass, network operators seek the convergence of command and control. These hubs of activity are prime targets, potentially presenting an enormous strategic benefit with relatively minimal risk to materiel.

Cyber is also not the full answer to resolving conventional asymmetries. A substantially weaker nation is not substantially more likely to achieve victory by simply applying force against a stronger enemy's networks. To effectively minimize adversary asymmetries by way of degrading their ability to

conduct joint warfare requires vast organizational efforts that are often beyond the reach of weaker nation. At the same time, traditionally potent actors such as the United States, Russia, and the People's Republic of China are all thoroughly leading offensive cyber doctrine. Instead of decreasing asymmetries, powerful actors could use offensive network capabilities to increase them. Weaker parties to conflict also have less resources to spend on network defense and secure development of military resources. That means they must rely on commercially available solutions, imported military equipment, and aging hardware. As a result, such parties may find themselves on the receiving end of persistent network attacks rather than effectively delivering them.

A trinity of traditional military concepts – surprise, deception, and destruction – is enlightening. Tracing their origins back to the earliest days of warfare, network operations are intrinsically geared towards surprise and deception. Extensive prepositioning of operational assets and the ability to subtly manipulate software and sensors are conducive to the same principles of subterfuge offered by Sun Tzu. As hardware destruction by way of software attacks is difficult, the metrics must simply be calibrated to account for digital destruction and physical disruption. These can be accomplished at unprecedented scale, yielding effects ranging from small tactical disturbances to widescale strategic disruption of capacity to operate.

Offensive network operations are immensely useful to all manner of operations, to aggressors both disadvantaged and dominant. It is the discourse that counts; the involvement of intelligence, network operators, weapon developers, military command, battlefield staff, and policy makers is mandated to create effective doctrine. By separating the capabilities to event and presence based, it assists in overcoming several existing issues, yet others will remain. Overcoming challenges is a long and arduous process, but one that can potentially result in a force multiplier effect across all aspects of conflict.

5. American Cyber Superiority

Overview

In the twentieth century the United States had led the charge in technology-enabled military strategy. It had culminated in the 1991 Gulf War, viewed with surprise and consternation by global adversaries who realised the discrepancy between US technological prowess and their own. Even as other global powers acquired increasingly advanced technologies, the capability to target information networks at scale seemed a distinctly US advantage. Information leaked from several high-profile incidents shone a crucial light at how developed the US technological capacity to wage network warfare truly is; developing offensive platforms, encroaching on adversary networks, researching equipment used by enemies, and creating subtle yet significant effects. Yet as before, the US has led by technology rather by strategy; the former continues to precede the latter, creating mismatched capabilities and a lack of coherence on how to achieve goals with MONOs.

Documentation on the US approach to "cyber" as an operational space is vast. It includes policy directives, national strategy documents, doctrinal publications both general and service-specific, and significant coverage of various programs advancing MONOs as means to generate effects. Alongside publications, private-sector research has uncovered several network intrusion campaigns commonly associated with the US, including toolsets presumably employed by the NSA, CIA, and elements of the military. Overall, US coverage of all matters cyber offers a rare, unique glimpse into the evolution of a discipline within the US military. This affords a critical overview of both high and low points of the US approach to network operations.

The US de-facto leads the school of thought envisioning "cyber" as an independent combatant domain. The domain approach entails observing all efforts to attack and defend networks as doctrinally and operationally distinct from the other – physical - domains. While US doctrine clearly and loudly identifies the interdependence between networks and the physical domains, it maintains that the former requires separate command from the latter. These efforts have resulted in an intricate amalgamation between cyber, electronic warfare, and information operations in which it is unclear where one begins and the other ends due to the numerous overlaps between the three disciplines. The American approach has both advantages and disadvantages, but could nevertheless benefit from the distinction between event and presence-based capabilities to provide commanders with options while retaining the strategic sensitivity of presence-based operations.

A 2015 Defense Science Board (DSB) report highlighted the dangers of lumping all MONOs under the same framework. The report definitively stated that "…the United States must maintain – and be seen to maintain – an array of scalable offensive cyber capabilities – including high-impact strategic

cyber attack options – as an integral part of its cyber deterrence posture[472]." The DSB conflated the robustness of a partly-visible event-based attack capability and strategic presence-based capabilities that must inherently remain covert. The report then claimed that "Unlike precision-guided munitions, cyber weapons cannot be bought and deployed on a delivery system… with confidence that they will work when needed. A highly talented cadre of cyber warriors must work together closely with intelligence specialists and technologists in a highly classified environment[473]." This remark disregarded the potential of utility of deployable event-based capabilities which already exist within the US arsenal, while assuming that all MONOs must remain under the purview of remote operators within intelligence units.

This chapter will present the argument that *the US is technologically well-positioned to conduct MONOs, but a rigid approach to cyber as a domain limits effective integration*. The United States has both the operational experience, technical expertise, and high-quality intelligence required to be consistently successful in employing MONOs. Simultaneously, a reoccurring predilection for a technology-first strategy means that capabilities are often created as detached from considerations of need or the requirements of the forces who may eventually employ them. A well-developed, co-opted national defence industry is fully capable of crafting packaged event-based capabilities that could then be delivered to deployed forces. At the same time, The National Security Agency has provable experience both operationally in penetrating hard-to-reach network targets and developing advanced presence-based capabilities that could then create effects against them. Yet both have traditionally struggled in transparently delivering capabilities to the parties who need them based on a thorough understanding of the threats and opportunities. Bridging these challenges by shattering some of the existing boundaries between cyber and the other domains could position MONOs as contributing value across the spectrum of military operations.

Even more so, the relatively advanced US approach to MONOs means that second-order integrations may be a viable reality. These include using MONOs to enable or deliver other network operations rather than just support kinetic forces and attacks. Event-based capabilities and their presence-based counterparts could work in tandem by having one facilitate the other, yet that requires an intimate familiarity with the characteristics of each, and an established trust between forces and their available capabilities.

Separation by Doctrine

The US approach to network warfare is one of the most publicly accessible. With experience in targeting digital communication that spans decades, US strategists have increasingly recognised the utility of pursuing networks to accomplish a broad spectrum of objectives ranging from limited tactical effects to broad strategic success. Mounting US attention to the operational significance of networks famously resulted in the 2009 creation of Cyber Command, and later in its mid-2018

[472] Defense Science Board, "Task Force on Cyber Deterrence" (Department of Defense, February 2017), 14.
[473] Defense Science Board, 14.

elevation to a full "unified combatant command" thus recognising its importance towards US strategic success[474]. Even as the Pentagon dramatically reflected at the time of elevation that "the cyber domain will define the next century of warfare", the specifics of how the US seeks to accomplish this are worth examining in depth.

American thoroughness has resulted in laboriously crafted doctrinal maturity, enabling operating forces to potentially integrate a vast array of capabilities. The linchpin of US network warfare doctrine is Joint Publication 3-12: Cyberspace Operations, a core document providing some of the standard definitions, objectives, and approaches all US forces are expected to implement and adhere to[475]. It is important however to note that a more complete reconstruction of US doctrine and strategy for MONOs can only be accomplished by reviewing other relevant documents, policy directives, committee hearings, technical specifications of capabilities, and leaked classified materials.

Operating against networks is formulated in the broader context of a new US strategy for victory in modern conflict. This approach is perhaps most commonly presented as "Multi-Domain Battle", an integrative strategy heavily favouring joint operations across multiple warfighting domains, incorporating asymmetric capabilities and eschewing traditional direct combat. Modern US doctrine has accepted that technological advancements uniquely allow adversaries to challenge US forces where they were traditionally perceived as vastly superior[476]. Similarly, military strategy acknowledges the difficulties presented in overwhelming modern defences with directly applied force, a traditional strength of US forces in the last several decades. As written by the US Training and Doctrine Command (TRADOC); "The cost of penetrating prepared enemy defenses is now too great for current conceptions of forward positioning and expeditionary maneuvers to effectively deter adversaries and prevail in armed conflict[477]." This is precisely the type of challenge that MONOs may help ameliorate.

US strategies consider offensive network capabilities to be key in achieving objectives in modern conflicts. Contributions may be direct by actioning against a target, or by otherwise enabling conventional forces to accomplish their missions. The Department of Defense's previous 2015 Cyber Strategy already articulated this quite well as the aspiration to "build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all levels[478]." This in turn supports the notion that MONOs can have measurable contributions to commanders in various circumstances. Within US Cyber Command's mandate is

[474] U.S. Department of Defense, "Cybercom to Elevate to Combatant Command," accessed June 10, 2018, https://www.defense.gov/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/.

[475] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018.

[476] TRADOC, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040" (U.S. Army Training and Doctrine Command, October 2017), 4–5.

[477] TRADOC, 3.

[478] U.S. Department of Defense, The Department of Defense Cyber Strategy, 3.

similarly etched an understanding that they must "rapidly transfer technologies with military utility to scalable operational capabilities[479]."

The rich tapestry of US official documentation on MONOs indicates a comparatively firm grasp of the value that such capabilities may lend. Many of these were not originally intended to be publicly available. In 2013, NSA leaker Edward Snowden included several policy documents among the trove of materials released by him to media outlets. Principally relevant among those is Presidential Policy Directive 20 (PPD-20) on Cyberspace Operations. Cloaked in its intended classification, the document provided a candid view of some crucial aspects of operating in and against networks[480]. On the risk of uncontrollable cascading effects as a result of misusing MONOs, the document warns against "…cyber effects in locations other than the intended target, with potential unintended or collateral consequences that may affect US national interests in many locations[481]." On the need to selectively employ MONOs to avoid unduly risking brittle capabilities, the policy claims that an effort must be made to "…identify potential targets of national importance where [Offensive Cyber Effects Operations] can offer a favourable balance of effectiveness and risk as compared with other instruments of national power[482]." In respect to the possibility of attaining various levels of surprise and the spectrum of possibilities, the document provides a lucid articulation:

> *"[Offensive Cyber Effects Operations] can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from the subtle to severely damaging.[483]"*

There is a substantial measure of strategic wisdom to unpack in PPD-20. Even absent of details on how concretely MONOs may be employed, the document directly articulates several of the strategic contributions that they may have, as reviewed in previous chapters. Within three pages of content, the directive refers to the unique economy of force consideration offered by MONOs alongside the dangers of detrimental collateral effects that may occur by incorrectly employing them. Similarly, the above quotes indicate a desire to subvert conventional centres of gravity that are increasingly proving resilient to US technological prowess, instead opting for an indirect approach that may carve a path towards coercing an adversary. Considering the seemingly limited battlefield use of MONOs by US forces to date and the decade-long focus of US forces on counter-insurgency in Iraq and Afghanistan, these observations are remarkably apropos.

US literature on doctrine and strategy is cascading. Documentation exists at the national level, which in turn leads to overarching integrated military doctrine, finally resulting in service-specific doctrine and strategy. Service-specific doctrine entails translating the broad criteria set at the higher

---

[479] U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," March 23, 2018, 8.

[480] PPD-20 has supposedly been revised in August 2018 by the Trump administration, in a bid to loosen restrictions on MONOs. See Eric Geller, "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand," *POLITICO*, August 16, 2018, https://politi.co/2MSWCnS.

[481] United States Government, "Presidential Policy Directive 20 - U.S. Cyber Operations Policy," October 2012, 6.

[482] United States Government, 9.

[483] United States Government, 9.

levels and extracting potential utility for service objectives. The Army would not operate under the same conditions as the Air Force, Navy, or Marines. Each have their existing concepts of operations (CONOPS), platforms, and procedures. It is in the service-specific doctrines where we observe the US at its best; the multiple layers of integrations are indicative of a comprehensive push towards having more MONOs be made available for combat missions.

The aforementioned JP 3-12 doctrinal document exemplifies both the strengths and relative weaknesses of the US posture on MONOs. Chiefly hampering overall clarity is the odd relationship between "cyberspace", the electromagnetic spectrum (EMS), and information. As US capabilities deepen across the three categories, the lines between them appear increasingly blurry and the attempts at distinguishing between them laboured. While the document stipulates that "Cyberspace is wholly contained within the information environment[484]", only the former is defined as a distinct domain while the latter is relegated to a separate publication[485]. Electronic warfare is shunted even further away as a sub-publication of information operations[486]. This is particularly puzzling, as Joint Publication 3-13.1 on Electronic Warfare contains the following accurate qualification:

> *"Since cyberspace requires both wires and wireless links to transport information, both offensive and defensive cyberspace operations may require use of the [electromagnetic spectrum] for the enabling of effects in cyberspace. Due to the complementary nature and potential synergistic effects of [electronic warfare] and computer network operations, they must be coordinated to ensure they are applied to maximize effectiveness[487]."*

The dependency between the EMS, networks, and information is unbreakable. They are wholly dependent on one another as they merely represent different layers of the same communication model. In a positive indication of progress, US doctrine does indeed reflect the multi-layered approach to networking, though somewhat sub-optimally. Joint Publication 3-12 outlines the "cyberspace layer model" as comprised of three layers; a physical network layer encompassing physical hardware, terrain, and transmission medium; a logical network layer that refers to the links and networks that make up "cyberspace"; and the cyber-persona layer which reflects the actual use of information. This is useful to a degree, but may not serve to fully decouple networks, the EMS, and information[488].

Within the services, the Army's implementation of network warfare is novel. Coalescing all under "Cyberspace electromagnetic activities", or CEMA[489], the Army has recognised the natural relationship between the electromagnetic spectrum as the medium, cyberspace as the networks, and information as the payload. The Army doctrine manual on the topic acknowledges both opportunity and risk, advantages and disadvantages, and how these broadly manifest, thereby offering a cautious but

---

[484] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, 27.
[485] U.S. Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," November 20, 2014.
[486] U.S. Joint Chiefs of Staff, "Joint Publication 3-13.1: Electronic Warfare," February 8, 2012.
[487] U.S. Joint Chiefs of Staff, 11.
[488] U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, 22–24.
[489] While the US Army is the primary organ within the US armed forces to use CEMA as a viable term, it now features prominently in doctrinal publications in other Western forces. See for example UK Ministry of Defense, "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities" (UK MoD, February 2018).

optimistic vision as to what could be done with such capabilities both against US adversaries and against US assets[490].

The Navy found itself rapidly orienting to a new reality. In 2013, the service discovered a significant breach of their unclassified networks and immediately began investigation and remediation[491]. Under the operational moniker "Rolling Tide", Navy network operation teams sought to cleanse Navy networks of foreign presence. Indicative of their perception of the intrusion, Fleet Cyber Commander Vice Admiral Tighe used combat vernacular to describe their experience; "we… fought through an adversary intrusion into Navy's unclassified network[492]." In essence, the Navy viewed Rolling Tide as countermeasures to a presence-based operation. Despite the intrusion focused on unclassified – and thereby largely non-operational – networks, the Navy consequently initiated deep internal reforms intended to better orient it towards cyber operations[493] both defensive and offensive. In subsequent public content, the Navy presented its strategic plans to defend its own assets from network attacks, tacitly confirming both presence and event-based attack vectors that must be mitigated[494].

The Air Force doubled down on its framing of cyber as an independent domain and separated its activities into distinct commands within the service. Air Force Policy Directive 17-2 on Cyber Operations lists the requirements to "…execute Cyberspace Operations to support the joint warfighter requirements, increase effectiveness of its core missions, increase resiliency, survivability and cybersecurity of its information and systems, and realize efficiencies through innovative [Information Technology] solutions[495]." This definition encompasses both offensive and defensive network operations, with limited language on how those could apply towards achieving these broad objectives. The 24th Air Force appears largely responsible for defending dedicated Air Force networks, but also training and preparation of "ready forces" in what ostensibly includes limited event-based capabilities. Conversely, Joint Force Headquarters – Cyber is responsible for execution of strategic offensive cyber capabilities authorised by the Secretary of Defence or the President, suggesting responsibility over presence-based capabilities[496].

The Department of Defense's vision for cyberspace remains rigid and brittle. Envisioning "cyberspace" as a well-defined domain may initially appear promising as an approach towards lending clarity to an evolving doctrine. Yet, it results in a malleable reality incongruent with the department's desires; cyberspace, electronic warfare and information operations all routinely bleed into one another within US doctrine. The result is inconsistent application and a distinct lack of transparency from warfighters on how to best operate within the new domain. Numerous parties share

[490] U.S. Army, "Army Field Manual 3-12: Cyberspace and Electronic Warfare Operations" (US Army, April 2017).

[491] Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers," *Wall Street Journal*, September 27, 2013, sec. World, https://www.wsj.com/articles/us-says-iran-hacked-navy-computers-1380314771.

[492] Edward Cardon et al., "Cyber Operations: Improving the Military Cybersecurity Posture in an Uncertain Threat Environment," § Committee on Armed Services House of Representatives (n.d.), 5.

[493] Cardon et al., 6.

[494] Troy Johnson, "Navy Cyber Resilience" (June 6, 2016).

[495] U.S. Air Force, "Air Force Policy Directive 17-2: Cyberspace Operations," April 12, 2016, 2.

[496] U.S. 24th Air Force, "Commander's Strategic Vision" (US Air Force, March 8, 2017), 1.

responsibilities for ensuring operational success. Cyber Command has sweeping domain oversight; service cyber commands concentrate domain-specific integrations of network capabilities; geographic commands maintain ownership of joint operations within their theatres and the specific assets who carry them out; and the NSA retain the actual sources, technical and operational capabilities, and discipline required to generate adversary network effects. Activation of some MONOs requires presidential approval communicated by the secretary of defense[497]. While the requirement to do so is repeatedly mentioned in US doctrine[498], It is immensely difficult to deconflict so many parties even in the best of circumstances[499]; it is doubly so for a domain almost wholly characterised by sensitive, compartmentalised offensive capabilities.

An overly firm bureaucracy may stifle the agility required to optimise military value from MONOs[500]. Boundaries on network operations are concurrently too vague and too strict, with the Trump administration's 2018 bid to loosen restrictions on MONOs currently having an unclear impact[501]. As a result, misunderstandings of their operational parameters may curtail a desire to use them or even the grasp of when they would contribute unique value. As McGhee articulated well in 2016; "Ambiguous definitions that lead to a lack of understanding of cyber utility exacerbate the disconnect between offensive cyber operations and kinetic operations… We do not necessarily understand what those definitions mean, because they are not well defined[502]."

The adherence to cyber as a domain is perhaps the key element which separates the US from its near-peer adversaries. The distinction between electronic warfare, information operations and cyberspace is fuzzy beyond the point of usefulness. It is unclear when does an EW platform defeating an adversary system by transmitting a digital payload qualifies as a cyberattack. It is similarly unclear if a MONO manipulating adversary propaganda in a war zone qualifies as a cyber operation or an information operation. It is unclear because these distinctions are often artificial. All MONOs are dependent on the electromagnetic infrastructure carrying data. The network effects employed almost always directly impact information in some form – either by corrupting it, manipulating it, preventing access to it, or otherwise occluding its intended use. The three-way interplay between the electromagnetic spectrum, networks, and information must be a core aspect of the fundamental approach.

EVENT-BASED CEMA

[497] U.S. Department of Defense, The Department of Defense Cyber Strategy, 5; James E McGhee, "Liberating Cyber Offense," *Strategic Studies Quarterly*, Winter 2016, 47–48.

[498] See for example U.S. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," May 2, 2013, 12.

[499] Though such deconfliction pipelines certainly exist – see U.S. Department of Defense, The Department of Defense Cyber Strategy, 14., and they are elaborate. Some evidence indicates oversight from Cyber Command and operational control from the NSA, with activities carried out by deployed remote operations centres (ROCs), see NAVIOCOM Maryland, "NIOC Maryland Advanced Computer Network Operations Course," (n.d.), 11.

[500] In its 2018 national security strategy, the DoD has broadly stated that it must "…improve integration and agility" overall, see U.S. Department of Defense, "US National Security Strategy," December 2017, 32..

[501] Geller, "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand."

[502] McGhee, "Liberating Cyber Offense," 52.

The US military holds all the pieces required to successfully use event-based operations. It trains and forward-deploys operators meant to augment kinetic capabilities with MONOs. It develops advanced platforms intended to both deliver network payloads and simplify their use. The US enjoys dominance of the technological landscape alongside a highly capable intelligence apparatus, thereby supporting the elaborate operational lifecycle required. It is likely that some high profile operations – particularly ones involving special forces – incorporate such capabilities to a degree. Yet, a systemic incorporation of MONOs across the spectrum of joint operations remain lacking.

The divergent approach to MONO doctrine within the various US services means that implementation varies greatly. While the Navy and Marines publicly focus on primarily defensive measures, the Air Force demonstrates an evolved willingness to carry out strategic offensive network missions within its mandate. Yet, the one service currently indicating a desire to broadly incorporate event-based operations is the Army, as represented by the aforementioned CEMA doctrine[503]. Folding network activity into electromagnetic spectrum operations and electronic warfare strongly suggests a recognition that the practices bleed into one another and could therefore benefit from the synergy afforded by their combination. As a result, the US Army stands out as relatively mature in its doctrinal approach to event-based operations.

The Army is currently exploring how to best extract operational value from network operations. Efforts have ratcheted up largely due to the realisation that after a year of counter-insurgency operations against poorly equipped adversaries, the US is woefully underprepared to tackle near-peer adversaries in electronic warfare and battlefield network operations[504]. Yet even as the Army searches for solutions, it remains hamstrung by the military-wide reality stating that "current authorities and policy on offensive cyber capabilities and effects are governed by the highest levels of government[505]." This perception emanates from sensitive presence-based operations and lumps all MONOs together, limiting the Army's capacity to own operational capabilities that could then be integrated. More nuance and distinction between event-based and presence-based capabilities at the doctrine level could afford the Army firmer boundaries to seek capabilities within, thereby generating opportunities that do not require top-echelon approvals. Even as they struggle to map out the various possibilities of MONOs, the Army identified networks as an adjacent and dependent space to the electromagnetic spectrum. At the deployed force level, this could mean event-based capabilities targeting adversary infrastructure, weapon platforms, and communication networks.

Despite doctrinal difficulties, the multi-decade prominence of the NSA as a top provider of signals intelligence uniquely positioned US forces to both acquire a deep understanding of adversary systems and provide potential reach where it would otherwise be difficult to acquire. Persistent tapping of data arteries within the global internet grid and sensitive adversary networks means that event-based

[503] U.S. Army, "Army Field Manual 3-12: Cyberspace and Electronic Warfare Operations."

[504] Mark Pomerleau, "US Is 'Outgunned' in Electronic Warfare, Says Cyber Commander," C4ISRNET, August 10, 2017, https://www.c4isrnet.com/show-reporter/technet-augusta/2017/08/10/us-is-outgunned-in-electronic-warfare-says-cyber-commander/.

[505] Mark Pomerleau, "Here's How the Army Wants to Integrate Cyber, EW into Operational Formations," Fifth Domain, October 2, 2017, http://www.fifthdomain.com/dod/army/2017/10/02/heres-how-the-army-wants-to-integrate-cyber-ew-into-operational-formations/.

operations may be carried out against these without ever introducing a presence component. Injection of traffic to block, manipulate or otherwise influence data streams could be a crucial vector towards impacting adversary networks. This may manifest in programs similar to the now-exposed NSA QUANTUMTHEORY project, which "…dynamically injects packets into a target's network session to achieve CNE/CND/CNA network effects[506]." Packet injection allows an adversary to externally splice data into networks that may otherwise be inaccessible, thereby manipulating or compromising them.

These capabilities often have steep intelligence requirements. Crucially, the documentation for QUANTUMTHEORY specifically called out the incorporation of passive signals intelligence (SIGINT) in targeting[507], thereby indicating the capacity to conduct high-resolution targeting as required for such capabilities to be employed judiciously. The need for tight support from operational intelligence for effective MONOs was also referenced in the NSA's Sentry Eagle program, in which the NSA "…provides SIGINT that supports the planning, deployment/emplacement and employment of [Computer Network Attack] combat capabilities[508]."

Abilities may at times only be useful if their usage pipelines are heavily streamlined. Communication is key; battlefield commanders must be made aware that a capability exists and the circumstances around its optimal use. One such example may be in event-based capabilities such as QUANTUMSKY – which facilitated disruption of web access – or QUANTUMCHOPPER – which enabled disruption of file transfers[509]. Seemingly tactical capabilities, they could still prove advantageous to deployed forces in certain scenarios. Yet, the documentation around these belies their internal sensitivity, thereby suggesting that they were reserved for strategic operations or compartmentalised special activities. It is unclear if comparable capabilities were or are available to support regular deployed forces.

Both 2016 and 2017 were painful years for the US intelligence community. A series of intrusions against institutions embodying national sovereignty such as the Democratic National Committee (DNC) reflected the vulnerability of the United States to outside intervention by way of information operations. These breaches were accompanied by data stolen from the NSA, CIA, and other leading agencies, weighing down public trust in the institutions and inflicting damage on the US capacity to conduct MONOs effectively. The grand theft of NSA data presumably originated from a group calling itself "The Shadow Brokers"[510], while the CIA content was leaked directly to Wikileaks where it received the codename "Vault 7"[511]. An additional leak from the NSA – the contents of which not

[506] NSA, "Getting Close to the Adversary: Forward-Based Defense with QFIRE," (June 3, 2011), 7.
[507] NSA, 2.
[508] NSA and USSTRATCOM, "National Initiative Protection Program - Sentry Eagle," November 23, 2004, 8.
[509] NSA, "Case Studies of Integrated Cyber Operation Techniques," (2011), 13.
[510] The Shadow Brokers are suspected as at least partially affiliated with the Russian government, see James Risen, "U.S. Secretly Negotiated With Russians to Buy Stolen NSA Documents — and the Russians Offered Trump-Related Material, Too," *The Intercept* (blog), February 9, 2018, https://theintercept.com/2018/02/09/donald-trump-russia-election-nsa/.. For coverage of their public communications and content, see Comae, "The Shadow Brokers: Cyber Fear Game-Changers" (Comae Technologies, July 2017).
[511] The files can be found at the Wikileaks site, see Wikileaks, "Vault 7: CIA Hacking Tools Revealed." The individual behind the Vault 7 leak was eventually revealed to be former CIA software engineer Joshua Schulte. There is no indication that he was knowingly working in the service of a foreign government at the time. See Adam Goldman, "New Charges in Huge C.I.A. Breach Known as Vault 7," *The New York Times*, June 19, 2018, sec. U.S., https://www.nytimes.com/2018/06/18/us/politics/charges-cia-breach-vault-7.html.

publicly disclosed – was traced to NSA contractor Harold Martin[512]. The aggregate leaks shine a partial spotlight on many US presence and event-based capabilities.

The capacity to remotely compromise systems is instrumental to all MONOs. Specifically, in event-based operations where the attacker is presumed to not have the time nor the capacity to conduct a long, cautious targeting campaign, a solution is necessary that would rapidly succeed with a high probability rate. Within the Shadow Brokers leak, the EternalBlue tool was a coveted exploit enabling wormable remote code execution, thereby allowing cascading automated compromise of vulnerable Windows-based systems[513]. The exploit – one of several in the same family and numerous others of differing quality in the Shadow Brokers leak – soon became the lynchpin component in several high-visibility malware campaigns such as WannaCry and NotPetya, notorious for their unusual virulence and destructive impact on affected systems and networks. While both self-identified as financially motivated ransomware, they were soon attributed to the North Korean[514] and Russian[515] governments respectively, thereby becoming de-facto cascading event-based capabilities.

Incorporating MONOs into military hardware for battlefield use is an arduous process. It requires significant research and development resources, intimate collaboration with intelligence agencies providing required telemetry, a trust relationship with combatant forces resulting in coherent, realistic enumeration of requirements, and a deep understanding of the operational lifecycle into which these capabilities may eventually integrate. For this purpose, the US military-industrial complex is uniquely qualified. Companies such as Lockheed Martin, Raytheon, and others enjoy close relationships with their in-service peers and the wherewithal required to develop platforms over numerous years. While the vast majority of technologies remain understandably classified, a glimpse into some publicly filed patents reveals just how prominently they feature throughout the MONO lifecycle for event-based capabilities.

Perhaps the best-known instance of field-worthy event-based capabilities is the EC-130 Compass Call aircraft. Originally deployed in 1981, later evolutions of the aircraft have also demonstrated the capacity to directly target networks. As cheerfully explained by Major General Burke Wilson of the US 24th Air Force in 2015; "Lo and behold! Yes, we're able to touch a target and manipulate a target, [i.e.] a network, from an air[craft][516]". The Compass Call's onboard equipment facilitating these new capabilities is provided by British defence contractor BAE. This is significant, as BAE is purportedly behind the Suter event-based platform previously referenced in this thesis. As such, this indicates a

[512] Martin reportedly hoarded over fifty terabytes of classified data. Despite a chronological correlation, he was never publicly linked to the Shadow Brokers. See Scott Shane, "Ex-N.S.A. Worker Accused of Stealing Trove of Secrets Offers to Plead Guilty," *The New York Times*, January 1, 2018, sec. U.S., https://www.nytimes.com/2018/01/03/us/politics/harold-martin-nsa-guilty-plea-offer.html.

[513] Microsoft, "Microsoft Security Bulletin MS17-010 - Critical."

[514] UK Foreign Ministry, "Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks," GOV.UK, December 19, 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

[515] U.S. Press Secretary, "Statement from the Press Secretary."

[516] Freedberg Jr., Sydney J., "Wireless Hacking In Flight: Air Force Demos Cyber EC-130," *Breaking Defense* (blog), September 15, 2015, https://breakingdefense.com/2015/09/wireless-hacking-in-flight-air-force-demos-cyber-ec-130/.

long-term dedication from BAE towards providing the US and its allies with robust platforms to conduct battlefield MONOs.

Autonomous platforms are likely to feature heavily in US event-based capabilities. One such example is a 2016 patent submitted by Selex Galileo, an offshoot of defence company Leonardo dedicated to providing solutions to the US Department of Defense[517]. The patent details a dedicated unmanned aerial system (UAS) small enough to evade detection by air defence systems and designed specifically to deliver electronic warfare and event-based attacks, reducing the risk to manned assets and paving the way for kinetic attacks. The drone documentation reveals the desire to deliver "…[radio frequency] based cyber effects[518]". This is the quintessential manifestation of an event-based capability as an evolved electronic warfare attack vector, one that simply seeks to target a platform by attacking its software rather than its sensors.

Other technologies encapsulate the spirit of event-based operations, even if they do not recognise it as such. Various elements within the US military have increasingly begun to adopt the use of Digital Radio Frequency Memory (DRFM)[519]. The technology allows the rapid recording, digitization, manipulation and retransmission of electromagnetic signals so that they could be weaponised against an adversary in a form of evolved jamming. The transmission itself can be modified on the digital level, potentially generating different effects. This form of jamming thoroughly blends electronic warfare with MONOs, as transmissions affect adversary platforms on the software level rather than on the sensory level. This natural escalation results in far more substantial flexibility and the ability to manipulate targeted systems at a high level of accuracy, creating effects previously impossible. Manipulation of the digital payload within a signal can result in the creation of altogether new information, increasing the range of options available to the commander using the ability.

Raytheon predominantly features as a provider of MONO-related technologies. In one 2014 patent partially titled "Digital weapons factory[520]", Raytheon claims to be able to dynamically match an offensive network payload by assessing the targeted adversary equipment[521] in near-real time. This pairing is done transparently to the operator, thus saving them the otherwise steep requirement for familiarisation with MONO techniques normally denied to fielded forces. Presumably, the technology calculates a probability of success and only upon passing a threshold would an offensive tool be created for use. A similar yet more specific 2014 Raytheon patent attempts to tackle ballistic missile defence (BMD) by outlining a system that can assess the vulnerabilities of a launched missile and attempt to pair a viable event-based capability to defeat it[522]. This is mirrored by a subsequent 2017

[517] Matthew Keegan and Stephen Leonard Engelson Wyatt, Method and system for a small unmanned aerial system for delivering electronic warfare and cyber effects, United States US20180009525A1, filed March 15, 2016, and issued January 11, 2018.

[518] Keegan and Wyatt.

[519] John Keller, "Navy and Air Force Choose DRFM Jammers from Mercury Systems to Help Spoof Enemy Radar," Military & Aerospace Electronics, June 18, 2014, https://www.militaryaerospace.com/articles/2014/06/mercury-drfm-jammer.html.

[520] Paul C. Hershey, Robert E. Dehnert JR, and John J. Williams, Digital weapons factory and digital operations center for producing, deploying, assessing, and managing digital defects, United States US9544326B2, filed January 20, 2015, and issued January 10, 2017.

[521] The patent documentation specifically notes a missile or a tank as viable scenarios of use.

[522] Paul C. Hershey, Joseph O. Chapa, and Elizabeth Umberger, Methods and apparatuses for eliminating a missile threat, United States US20160070674A1, filed September 9, 2014, and issued March 10, 2016.

Raytheon patent detailing an integrated kinetic, electronic warfare and MONO-delivering system[523]. These technologies – if functional - can afford tactical agility which may then be realised in field scenarios. Bridging the gap between MONO subject matter expertise and combat forces could make event-based operations far more likely to be used routinely in the field.

Other patents attempt to simplify the overall battlefield awareness and direction of MONOs. Recognising that it is often difficult to grasp aspects of intangible warfare and doubly so with battlefields becoming increasingly saturated with various networks, these technologies seek to streamline the process. In one patent from Boeing, a technology is offered to orchestrate both "cyber" and electronic warfare missions[524]. An older Raytheon patent tries to similarly assist by directly offering "command and control systems for cyber warfare[525]". These technologies prove how an investment in the preparation phase of the operational lifecycle can then reduce overhead in the engagement, presence, and effects stages. By instrumenting all of those through a single unified platform, commanders can focus on how best to use the ability rather than the intricate characteristics of doing so.

Presence-Based Operations

The United States is arguably the best positioned entity to conduct high quality presence-based operations at scale. Supply-chain compromise, infiltration of third-party providers, cooperation from popular global service providers, and a range of zero-day exploits against widely used products enable access to a wide range of adversary networks. As before, available evidence points to a high capacity to conduct operations in service of an overall national security agenda, yet it remains unclear how thoroughly these capacities are made available to military planners. A review of leaked, disclosed, and publicly researched evidence is useful towards constructing the unusually rich tapestry of US offensive capabilities.

The majority of available data pertaining to US network intrusion originates with the National Security Agency. In its historic role as the premier provider signals intelligence, it had since organically and gradually grown into its mandate as the primary caretaker of US computer network operations (CNO), which encapsulates defensive, intelligence, and offensive efforts against adversary networks. Under that mandate, it had been incredibly prolific at creating capabilities and compromising key US adversaries, ostensibly for the purposes of answering critical intelligence requirements within its area of responsibility. Unfortunately for the agency, its allies, and the US at large – a series of leaks and compromises of the infrastructure, tools, and documentation it uses to facilitate CNO resulted in an inordinate amount of public scrutiny. Rather uniquely, the world was

[523] Paul Christian Hershey et al., System and method for integrated and synchronized planning and response to defeat disparate threats over the threat kill chain with combined cyber, electronic warfare and kinetic effects, United States US20180038669A1, filed February 28, 2017, and issued February 8, 2018.

[524] Seth L. Jahne et al., Techniques Deployment System, United States US20150369569A1, filed June 24, 2014, and issued December 24, 2015.

[525] Jonathon P. Leibunguth, Command and Control Systems for Cyber Warfare, United States US20090249483A1, filed March 30, 2009, and issued October 1, 2009.

given a partial yet surprisingly deep look at how a clandestine intelligence agency sought to weaponise networks and information.

It is crucial to note that the NSA does not operate solely under a direct military mandate and is primarily subordinate to its designation as an intelligence agency. As such, it is not tasked with directly accomplishing military goals, and is consequently often at odds when opportunities to conduct MONOs arise. As indicated by Ashton Carter in a previously mentioned text, despite the creation of Cyber Command – designed to remediate some of this tension and concentrate military network operation efforts – the NSA did relatively little to furnish the US military with MONOs at scale[526]. Instead, secrecy, bureaucracy and compartmentalisation mean that MONOs are heavily classified, known by relatively few, and deployable only for very specific pre-approved intentions approved by the highest tiers of US decision making. Yet irrespective of this and the limited signs of military offensive presence-based operations, previous network attacks carried out by the NSA are often an indication of overall US readiness to conduct them. Attacks that were carried out under the auspices of the NSA could theoretically be ported over to Cyber Command, where they would be employed according to military objectives and priorities. Perhaps the most well-discussed and visible of these sabotage operations is Stuxnet.

The Stuxnet malware targeting the Iranian nuclear project has been thoroughly scrutinised since its 2012 discovery. Even its purported operational designation as "Olympic Games" has been revealed in a New York Times article[527]. While as previously assessed this operation does not fully qualify as an act of cyber-warfare, it is certainly revealing as a presence-based operation that could be mirrored for military purposes[528]. A stealthy, modular capability incorporating dedicated attack components, and targeting a specific set of software and hardware used by an adversary wrapped in a self-replicating infection vector and several zero-day exploits, all indicate a tightly managed operational lifecycle. While a subsequent US capability in the vein of Stuxnet has not been publicly disclosed since, the tool remains a viable indication of US presence-based capabilities.

As previously indicated, deception is crucial towards maintaining the viability of a presence-based operation. Detection means mitigation, and subsequent decommissioning or revision of the attack tools. Importantly, Stuxnet maintained its deception even after commencing its effects phase[529], a decidedly unique feature enabling sustained – albeit reduced - impact against the target. Consequently, it was able to maintain continuous efficacy in a volatile environment, requiring a measure of operational nuance rarely found in other attack tools. Similarly, the self-propagation component of Stuxnet was coupled with code to detect specific hardware and software, thereby both identifying potential targets of interest while similarly avoiding harm against incidental infections [TKTK Richard Clarke: ""was that it very much had the feel to it of having been written by or governed

[526] Carter, "A Lasting Defeat: The Campaign to Destroy ISIS."
[527] Sanger, "Obama Ordered Wave of Cyberattacks Against Iran."
[528] See chapter two, where Stuxnet is shown to not meet the threshold of TIAGR as it was not conducted within the spectrum of military operations.
[529] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 25.

by a team of Washington lawyers"]. This attention towards limiting collateral effects is operationally significant both to defend the tool itself, but also prevent uncontrollable cascading effects that risk the overall mission or objectives. This manner of discipline is difficult to develop and doubly so to maintain, as evident in the eventual "break out" of Stuxnet which resulted in peripheral infections of ostensibly unrelated targets around the world[530].

Stuxnet was not enough. During the early years of the Obama administration – as Stuxnet was operating - the risk of a significant regional conflict in the Middle East peaked. Bolstered by conservative backing and a perceived sense of urgency, Israeli Prime Minister Binyamin Netanyahu reportedly became increasingly nervous. The illicit Iranian nuclear program, long suspected to have a military dimension, was rapidly advancing. Concern was growing in the US that additional viable solutions were necessary to deal with the Iran's nuclear aspirations that did not involve open warfare, in an attempt to reduce the likelihood of all-out war. A multi-target network attack seemed a potentially promising solution, one that could theoretically deliver success with minimal risk.

The plan for comprehensive strategic MONOs against Iran was reportedly folded into a program called "Nitro Zeus". In controversial coverage by New York Times journalist David Sanger, Nitro Zeus was described as essentially a series of presence-based operations against numerous critical targets, which Sanger claimed "…would have required piercing and maintaining a presence in a vast number of Iranian networks, including the country's air defenses and its transportation and command and control centers[531]." The operational plan behind Nitro Zeus suggested a schism in US thinking on network operations at the time; it was both ambitious enough to believe strategic coercion was singularly possible, while at the same time too narrow as to thoroughly integrate the capabilities into a broader military capacity. In this sense, presence-based MONOs were almost viewed as a strategic extension of special forces, one capable of surgical attacks on an unprecedented magnitude.

An additional nascent MONO capability can be found in a network espionage campaign dubbed "Slingshot" by researchers from Russian security company Kaspersky, who unmasked it. With forensic evidence indicating operational activity since at least 2012, the malware predominantly targeted Middle-Eastern and North-African nations. Defined as a high-quality versatile platform by the researchers, its truly unique differentiator was in the engagement phase of its operational lifecycle; the malware appeared to spread in part by exploiting vulnerabilities in network routers. Once it had successfully done so, Slingshot's operators appeared predominantly interested in harvesting intelligence from affected endpoints. Yet, having fully compromised its victims and with a capable, modular platform – a subsequent retasking could have turned Slingshot into a potent presence-based capability delivering a variety of offensive payloads.

---

[530] Falliere, Murchu, and Chien, "W32.Stuxnet Dossier," 6–10.

[531] David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict," *The New York Times*, February 16, 2016, sec. World, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Slingshot's most significant aspect is not the infection vector or its targeting; it is the context. State-sponsored network operations routinely get exposed by private sector research companies. More commonly then not, private sector analysis focuses on three aspects; (1) technical analysis of the malware and its components; (2) operational analysis of the threat actor's efforts; and (3), a victimology analysis of affected targets. Rather unusually, Slingshot's early 2018 reveal was rapidly followed up by a Cyberscoop article indicating that Slingshot was "…an active, U.S.-led counterterrorism cyber-espionage operation… used to target ISIS and al-Qaeda members[532]." The same article claimed the operation was under the purview of Joint Special Operations Command (JSOC), a subordinate part of US Special Operations Command (USSOCOM). The access and intelligence afforded by Slingshot was reportedly used to facilitate accurate targeting for kinetic operations. If supporting targeting was indeed the goal, it bolsters the notion that network operations are treated as part of the unique toolset provided mostly to US special forces.

On the technological side, Perhaps the quintessential case study is the NSA's "ANT Catalog". Leaked in 2013 by Edward Snowden, the catalogue purportedly originated from a subdivision of the NSA tasked with creating deployable hardware-software solutions for compromising networks[533]. Capabilities include access acquisition technology for firewalls, transmittable signals, mobile phones, servers, and personal computers. The now aging catalogue includes a highly classified bevy of solutions befitting different scenarios, thereby allowing the NSA's customers and partners to directly request a capability for operational use. The comparatively high level of technical details and manner of explanations suggest that the target audience was not strategic planners, but rather operational planners familiar with the tactical details of the adversary. Despite the restrictive classification, the very existence of a formalised network capability catalogue in 2009 suggests an evolved approach to incorporating these capabilities across various branches of the US defence establishment. If an equivalent catalogue is available to strategic planners detailing only the opportunities lent by such capabilities by using familiar military vernacular, it would likely encourage the co-optation of presence-based MONOs into the military operational lifecycle.

Evidence also points to the publicly analysed "Equation Group" threat group as being synonymous with the NSA's Tailored Access Operations (TAO) unit. In a 2015 report from Russian security company Kaspersky, the researchers discovering the group's activity and tools claimed it was "…probably one of the most sophisticated cyber attack groups in the world[534]." Within the same report, Kaspersky's analysis indicated evidence directly tracing the group's malware activity to 2001, with other anecdotal evidence suggesting some operational activity as early as 1996. If accurate, this positions the NSA as one of the most capable, persistent, and historically significant network operators in the world. The analysis similarly indicates that the malware in question employed several

[532] Chris Bing and Patrick Howell O'Neill, "Kaspersky's 'Slingshot' Report Burned an ISIS-Focused Intelligence Operation," *Cyberscoop* (blog), March 20, 2018, https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/.

[533] NSA, "ANT Product Catalog," 2009.

[534] GReAT, "Equation: The Death Star of Malware Galaxy," *Securelist* (blog), February 16, 2015, https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.

unique device persistence mechanisms[535], was remarkably stealthy, and sufficiently modular as to enable a wide array of payloads and capabilities. Some of the modules and exploits used by Equation Group were subsequently revealed in the aforementioned Shadow Brokers leaks, confirming the dazzling range of capabilities available to the NSA[536]. As such, the TAO's malware family was uniquely suitable for presence-based operations against a broad spectrum of global targets.

Occurrences of an integrated approach to cyber-warfare do exist. A relevant modern case for a joint kinetic-MONO strategy is versus the North Korean ballistic missile threat to the US. While volumes have been written on the threat itself, consensus broadly paints it as intricate and difficult to reliably overcome. Some of the parameters include wild fluctuations in the diplomatic relationship, a rapidly advancing ballistic missile program, and arguably nuclear payloads ready to be coupled onto warheads. The North Koreans have limited, tightly controlled internet access, reducing their online footprint and thus the available attack surface for MONOs. Conversely, a significant reliance on Chinese expertise, infrastructure and material support may also present opportunities. Increasing the likelihood of preventing a North Korean nuclear attack would require an integrated effort of all domains across the spectrum of operations. This entails a combination of kinetic ballistic interceptors, naval and air assets, electronic warfare, and presence-based operational capabilities. The layered approach can help ensure that even if multiple attempts fail, additional measures would be deployed in turn in a cascading fashion until they deplete or the threat has been mitigated.

The ballistic missile threat may be mitigated prior to an actual attack in an approach labelled "left of launch"[537]. The approach includes all efforts to defeat missiles by targeting the systems and components that make up their operational ecosystems. Rather than defeating the missile once launched, the goal is to prevent the launch or otherwise pre-emptively thwart its success. These efforts do not uniquely need to be MONO-based, as put forth by the Atlantic Council's Herbert Kemp;

> *"It is time to change the game from a purely defensive battle to one in which the fight is taken to the source – to attack the [Theatre Ballistic Missile] launch systems and their supporting infrastructures before missiles could be launched. All parts of the chain leading up to the launch event are potentially vulnerable to disruption or destruction, and the time is right to undertake a serious effort to engage the TBM threat 'left of launch'*[538]*."*

Left of launch operations presence a unique operation for a collaborative, full-spectrum US approach that incorporates pre-emptive attacks, supply chain sabotage, and presence-based MONOs. Indeed, each of these capabilities seems to exist separately and it is becoming increasingly clear that the US is determined to integrate these into a tiered defensive network. The Department of Defense outlined its approach in a 2017 declaratory memorandum; "The concept of operations for employing left-of-launch capabilities is set within the broader context of integrated offensive and defensive

[535] Resilience methods allowing a network intrusion tool to survive device restarts and attempts to remove it.
[536] Comae, "The Shadow Brokers: Cyber Fear Game-Changers."
[537] Left of launch references a timeline which places all actions prior to the launch on the left-hand, while post-launch mitigation attempts are right of launch.
[538] Herbert C. Kemp, "Left of Launch: Countering Theater Ballistic Missiles," Issue Brief (Atlantic Council, July 2017), 2.

operations for countering offensive missiles[539]." The department envisioned joint efforts to defeat missile threats by relying on varying capabilities including both kinetic and non-kinetic options.

Pursuing presence-based capabilities against the North Korean missile threat is compelling but challenging. While some reporters claim that such efforts have already manifested as an increased failure rate for North Korea's missile tests[540], proliferation researcher Jeffrey Lewis claims no credible evidence has been offered to support this notion[541]. Conversely, a 2015 panel of former US military staff officers on comprehensive missile defence[542] - later iterated by Andrew Futter in 2016[543] - offered that targeting ballistic capabilities with network operations risks undermining the certainty of classic nuclear deterrence models, thereby reducing overall security of all parties involved. The core characteristics of presence-based capabilities – that they are clandestine, difficult to track, and inconclusively effective mean that all involved actors cannot guarantee that either their defensive or offensive measures would be successful. This lack of transparency damages the clearly communicated notion of mutually assured destruction. Yet this lack of clarity similarly also means that nations may already be pursuing such presence-based capabilities, and arguably none are better poised to acquire them as the US.

Integrated Warfare

The US challenges in integrating "cyber" do not stem from a dearth of capabilities. A strategic investment in MONOs and network espionage tools over the last two decades have resulted in perhaps the broadest range of both presence and event-based capabilities globally. The possibilities are seemingly dazzling, including targeting critical infrastructure, dedicated military equipment, encrypted communications, industrial systems, and air-gapped networks. Targeting efforts span from entire countries to individuals in a collaborative effort that potentially includes thousands of staff across several agencies, units, and companies. The scope of US network operations is gargantuan.

Rather, the US challenges stem from a lack of focused offensive strategy, and a disconnect between the available capabilities and those who may use them most effectively. Deployed forces have limited support from event-based capabilities that could augment their operational lifecycles, and therefore cannot incorporate them into planning or rely on their availability when needed. Similarly, strategic planners are often disconnected from the scale and specifics of US network penetrations and capabilities, leaving only the highest of echelons with visibility into presence-based opportunities to inflict harm and facilitate success. US operators and units are likely capable of succeeding in both presence and event-based MONOs; it is the scaling aspect that remains lacking. Where many nations

---

[539] U.S. Department of Defense, "Declaratory Policy, Concept of Operations, and Employment Guidelines for Left-of-Launch Capability," May 10, 2017, 2.

[540] David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *The New York Times*, January 20, 2018, sec. World, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

[541] Jeffrey Lewis, "Is the United States Really Blowing Up North Korea's Missiles?," *Foreign Policy* (blog), April 19, 2017, https://foreignpolicy.com/2017/04/19/the-united-states-isnt-hacking-north-koreas-missile-launches/.

[542] Kenneth Todorov et al., Panel on Full Spectrum Missile Defense, CSIS, December 4, 2015.

[543] Futter, "The Dangers of Using Cyberattacks to Counter Nuclear Threats," *Arms Control Today* 46, no. 6 (2016): 8–14.

struggle to create capabilities, the US has them. It needs to do better at deploying them; it needs better doctrinal clarity.

The cycle of capacity acquisition could to be reversed. A separation into event and presence-based operations can assist in facilitating some of this process. If strategic planners were clear on the scope and possibilities presence-based capabilities lend, they could then task relevant capacity creators such as Cyber Command to create and maintain them. Persistent network intrusions are primarily facilitated by agencies such as the NSA for intelligence objectives, and subsequently weaponised if the necessity to do so arises. Introducing a presence-based operational mentality into the calculus would mean initiating intrusions with an offensive intent already in mind, thereby perhaps changing the approach, intrusion vectors, or even the toolsets used. Doing so may then allow a smoother offloading of access from the intelligence agency that created the access to the operational agency that seeks to attack the underlying targets. In a similar vein, a coherent plan to create and integrate event-based capabilities across all existing operational domains could result in force multipliers that deployed forces could rely on. As these capabilities would vary based on the region due to differing technologies and networks, they would need to be prioritised. A concerted, strategy-oriented push from acquisition planners in the Navy, Air Force, Marines, and Army could then solicit the sprawling US industrial base for event-based capabilities that would suit their requirements, rather than being approached by these companies with technologies as they come up with them. Technological innovation is crucial to success in modern warfighting, but only if it is channelled to meet requirements.

Beyond acquisition, the US is uniquely poised to use event and presence-based capabilities as force multipliers for each other, effectively creating hybrid MONO opportunities. While it is becoming increasingly clear that MONOs can enable kinetic operators, if the benefits of networks operations are sufficiently well developed and understood they could be used in support of each other. Opportunities in this space include using deployed event-based assets to breach networks and deliver presence-based malware that would subsequently be handed off to remote operators. Alternatively, networks compromised for presence-based operations may allow remote access to “air-gapped” networks, thereby facilitating follow-up event-based attacks against them. This would require painstakingly crafted bureaucracies and deconfliction channels that can rapidly decide how to jointly exercise multiple types of MONOs in mutual support. While this direction is implied in the latest iteration of US doctrinal literature[544], the reality is that such cooperation requires an intimate familiarity with the considerations on operating offensively in and against networks that still eludes the US military as a whole.

The notion that “cyberspace” is a domain remains a significant hurdle for this. Rather than viewing it as a distinct set of opportunities and capabilities, US military planners could benefit from increased integration, transparency, and seamless co-optation of networks into all aspects of operations. Networks are already integral to all other domains and would increasingly become so as technology progress and automation increases. The staggering US dependency on technology-led strategy would

[544] U.S. Joint Chiefs of Staff, “Joint Publication 3-12: Cyberspace Operations,” June 8, 2018.

only deepen if cyber is siloed in its own domain, relegating innovation and creativity in using MONOs to Cyber Command and its subordinate force structures.

Perhaps the greatest challenge that the US now faces is in amalgamating the progress achieved in implementing MONOs across its different services, agencies, and defence companies. Each contributes a crucial facet that arguably embodies desirable capabilities, were they to be integrated with one another. Both for event-based and presence-based capabilities, the US currently represents a reality where the whole is less than the sum of its parts, rather than the opposite. Even as the Army pursues CEMA it remains shackled to an overly broad doctrine that views all MONOs as a single sensitive operational approach. The Air Force does well to incorporate cyber as a notion but limits itself by relegating it to support roles as a domain of unique effects distinct from the airspace which it naturally commands[545]. The NSA has spent immense resources on developing both access and capabilities to action against critical targets that could prove strategic to future mission planning. And the US defence industry has proven innovative in fashioning event-based capabilities that could then be delivered from various platforms, integrated into the operational planning process, and translated to jargon and concepts familiar to military users.

The combination of these disparate approaches could result in a strategic advantage that rebalances the US against an increasingly contested geopolitical climate. Where near-peer adversaries such as Russia and China pursue advances technologies and MONOs of their own, the US already possesses them in a disjointed ecosystem that may fail to deliver effects when needed. Recognising that the electromagnetic spectrum, networks, and information are all different layers of the same man-made construct could help the US in distinguishing which entities should "own" which part of the overall effort. Whether or not it will do so remains to be seen, though the efforts towards an integrated conception of cyberspace continues across the US armed forces.

[545] This is echoed strongly in the words of the commander of the 24th Air Force, defining cyberspace as "a warfighting domain of operations where cyber operators generate effects differently than the ways we generate effects in Air, Space, Land and Sea.", see U.S. 24th Air Force, "Commander's Strategic Vision," 2.

6. The Russian Spectrum of Conflict

Overview

What was old is new again. Observing Russia's geopolitical disposition teases familiar themes reminiscent of Soviet thought. These include an increased belligerence characterised by friction with Western interests; diminishing cooperation with NATO and its contingent members; emphasis on austere national loyalty and an ever-present concern of NATO encroachment on its Western borders. Even as it is yet premature to claim a fully-fledged return to the dismal days of the Cold War where global stability seemed at a brink, global tensions between Russia and its historic rivals are on a notable incline.

The Russian geopolitical mentality is that of continuous strategic contest. Rather than envisioning clearly defined bouts of warfare capped at both ends by periods of peace, armed conflict is viewed simply a deterioration of existing relationships, either due to a perceived imminent threat or the pragmatic realisation of potential value to gain. This is a key notion within Russian strategic theory; envisioning warfare as a component part in a larger contest of will impacts their perception of conflict itself and the tools employed within it. Some tools that are deemed overly aggressive or even classically categorised as warfare by other nations may be designated as legitimate activities in Russian grand strategy.

This holistic perception of conflict has exasperated in the twenty-first century and is well articulated in Russian military thought. As Chief of General Staff Valery Gerasimov claimed in his seminal 2013 article; "In the twenty-first century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template[546]". Russian theorists such as Chekinov and Bogdanov describe what they call "a new-generation war", referring repeatedly to non-military actions before, during, and after armed hostilities ensue[547]. This conceptualisation of a new-generation war is echoed repeatedly both in Russian military theory and those who observe it, and offers some parallels to the controversial Western concept of "hybrid warfare"[548]. Adversarial actions bleed into the civilian sphere and draw on mass-media, psychological operations, academia, outreach, and diplomacy, months before armed conflict visibly erupts[549]. In this reality of diffused contest, discerning concrete elements of the Russian way of war may be challenging.

---

[546] Valery Gerasimov, "The Value of Science Is in the Foresight," *Military Review* 96, no. 1 (2016): 24.

[547] Sergey G. Chekinov and Sergey A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013): 12–23.

[548] Dmitry Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy* (Institut français des relations internationales, 2015), 21–23, http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

[549] Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 16–17.

This chapter will argue that *Russia has thoroughly integrated MONOs into a broader spectrum of information operations, but often fails to achieve objectives*. Drawing on decades of established doctrine, Russia has recognised and enshrined the usefulness of affecting information as a means of limiting or avoiding conflict altogether. Yet, technical and operational limitations have caused many operations to be exposed, while others were sub-optimally used or prematurely executed. As such, Russia has enjoyed relatively limited advantages from the use of MONOs, though it is comparatively poised to gain significantly from a more thoughtful approach.

There is a schism within Western analysis of modern Russian doctrine. While some evoke the notion of a new "Gerasimov Doctrine" which suggests a novel form of hybrid warfare, others are sceptical that these terms introduce meaningful value[550]. The label "hybrid warfare" is often used when describing the complexities of modern Russian strategy. Originally coined by Frank Hoffman in 2009[551], the underlying notion is that within the context of conflict Russia relies on a combination of multi-domain forces alongside non-military and irregular means of coercion. While this does indeed appear to be the case, there are noteworthy reservations preventing the term from being useful as a descriptor of Russian military behaviour. First, that the term is only applied to modern Russian doctrine implies novelty where it does not exist[552]. The observed "hybrid" approach to conflict is mostly a modern manifestation of the Soviet-era strategy for geopolitical competition. Second, it implies an intentional labelling from Russian military theory where there is no such effort. Much like when discussing cyber, the notion of hybrid warfare mostly exists within Russian literature when referencing Western commentary about it[553].

Russian grand-strategy often implements the idea of "reflexive control". Harkening to Soviet-era military thought[554], the concept calls for a gradual manipulation of an adversary's perception so that it organically begins to act against its own stated objectives[555]. This approach is thereby a subtler stand-in for classic coercive behaviour, which instead overtly seeks to compel an adversary to behave favourably. Reflexive control could manifest as either reshaping the information pipelines used by the adversary in the decision-making process, or manipulating actors of influence to generate more a more favourable setting[556]. The flexibility of the term embodied both the dynamic Russian approach to coercion but also their deep-set aversion to armed conflict where it was not necessary[557].

Reflexive control alludes to a grand strategy reliant on shaping truth to exert influence over a political adversary. While manipulating the flow of information has been an integral part of reflexive

[550] This includes Mark Galeotti, who inadvertently promoted and then railed against the use of the Gerasimov Doctrine as a concept. See Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* (blog), July 6, 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/..

[551] Frank G. Hoffman, "Hybrid Warfare & Challenges," *Joint Forces Quarterly*, no. 52 (2009): 34–47.

[552] Giles, "Russia's 'New' Tools for Confronting the West," 5.

[553] Charles K. Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (2016): 34; Giles, "Russia's 'New' Tools for Confronting the West," 9.

[554] Diane Chotikul, "The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study:" (Fort Belvoir, VA: Defense Technical Information Center, July 1, 1986), http://www.dtic.mil/docs/citations/ADA170613.

[555] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (June 2004): 237.

[556] Thomas, 242.

[557] Chotikul, "The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study:," 73–74.

control since the Soviet era, it has flourished in modern Russian grand-strategy. There are numerous similarities and overlapping areas between Russia's modern information operations doctrine and Soviet reflexive control[558], where both seek to manipulate perception and upset decision-making processes across all political and strategic levels. Thus, as previously examined with cyber-operations[559], there are well-established historical roots for the use of information campaigns to achieve objectives while pre-empting conflict.

There are several key characteristics in the overarching Russian approach to information and its uses. The first is that the entire information space is viewed as a fundamental aspect of modern geostrategic competition; this in turn explains the scale and investment in capabilities that target information in various ways. Second, there is little distinction between information operations and actual computer network operations. As the latter is wholly subsumed by the former, network operations are often not discreetly analysed. Third, electronic warfare – a traditional strength of the Soviets, is often viewed as on the same spectrum as its information counterpart. As a result, at least the potential to integrate MONOs across all disciplines is well-present in the current Russian order of battle[560].

Due to the holistic approach, network operations are often an indistinct component within the larger Russian information operations doctrine. Where Western doctrine often makes a comparatively clearer distinction between cyber-operations directly targeting networks and information operations that primarily tackle human perception, Russian doctrine views the information space as a continuous spectrum of operational capabilities[561]. These capabilities in turn serve a wide variety of purposes, many exceeding the military-strategic.

Russia does not just pursue reflexive control; it engages in *reflective strategy*. Many of its core principles stem from its own perception of threat, which in turn leads to adaptation of Western techniques and advantages[562]. Simply put, they often do to others as they fear will be done to them. Indeed, Russian theorists often view the Western and principally US agenda as bent on dismantling residual Russian influence. As colonel Maruyev claimed to this effect, "Obviously, the U.S. and its Atlantic allies are Russia's principal geopolitical enemy…[563]", later adding that "…as previously, the Americans will continue actively to foist their values on the rest of the world relying on all the force and assets available to them[564]."

---

[558] Maria Snegovaya, "Putin's Information Warfare in Ukraine," *Soviet Origins Of Russia's Hybrid Warfare, Washington*, 2015, 10; Franklin D Kramer et al., *Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework*, 2017, 11, http://www.atlanticcouncil.org/images/publications/Meeting_the_Russian_Hybrid_Challenge_web_0530.pdf.

Maria Snegovaya, "Putin's Information Warfare in Ukraine," *Soviet Origins Of Russia's Hybrid Warfare, Washington*, 2015, 10.[559] Snegovaya, "Putin's Information Warfare in Ukraine," 10; Kramer et al., *Meeting the Russian Hybrid Challenge*, 11.

[560] Dr Lester W Grau and Charles K Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces* (Fort Leavenworth: Foreign Military Studies Office, 2016), 289–90.

[561] Franke, "War by Non-Military Means," 14–15.

[562] Adamsky, *Cross-Domain Coercion*, 9.

[563] A. Yu. Maruyev, "Russia and the U.S.A in Confrontation: Military and Political Aspects," *Military Thought* 18, no. 3 (July 1, 2009): 2.

[564] Maruyev, 3.

While often blamed for engaging in prolific sub-warfare behaviour, Russian strategy has implemented this approach in part due to concerns of the United States aggressively pursuing the same[565]. To a degree, the renewed vigour in targeting the information space stems from the identification of a relative US technological advantage in the wake of the Gulf War[566], in which US Network-Centric Warfare (NCW) doctrine was fully on display. While some may argue that mirroring doctrine is a sign of strategic weakness[567], it can perhaps also be construed as a rare case in which a country proactively realigned its strategy to account for asymmetries. Russian military thought adapted Soviet concepts of dominating enemy perception to a modern, data-driven technological environment[568].

The Russian aspiration for information superiority cannot be stressed enough. Both in and out of conflict, Russia views perception across all levels and the information that shapes it to be a core tenet of its strategy. In the warfighting space, the military acknowledged that it lags far behind its Western counterparts and has commensurately sought to revitalise its position. This gradual yet enthusiastic investment included both a commitment by the military to invest in networked information systems[569] while simultaneously committing to engaging in offensive and defensive operations in the information space[570]. As with other aspects of its strategy, information operations do not have a branch of their own, and instead incorporate various elements from across disciplines and units[571]. As Giles notes, Russian's approach to information operations "…combines tried and tested tools of influence with a new embrace of modern technology and capabilities[572]."

The focus on information operations reflects an overall Russian aversion to overt armed conflict. As will be reviewed throughout the chapter, Russian grand-strategy aims to wield all available information tools to soften political adversaries, ideally to the point where conflict is altogether obviated. However, even if it remains necessary, such capabilities are meant to weaken resolve, sow discord, fragment alliances, and damage military readiness as to increase the chances of an offensive success and reduce its required duration. As Chekinov and Bogdanov colourfully write; "A new-generation war will be dominated by information and psychological warfare that will seek to achieve superiority in troops and weapons control and depress the opponent's armed forces personnel and population morally and psychologically[573]".

The result of the holistic, war-averse Russian approach is that most of their offensive activities in cyberspace do not separately meet the threshold of warfare. Russian activity may appear sporadic, low-intensity, half-baked or perhaps even crude when observed at the individual level. It is only when

[565] Bartles, "Getting Gerasimov Right," 32–33.
[566] Kramer et al., *Meeting the Russian Hybrid Challenge*, 4.
[567] Snegovaya, "Putin's Information Warfare in Ukraine," 9.
[568] Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 13.
[569] Col E A Perov and Col A V Pereverzev, "On the Prospective Digital Communication Network of the RF Armed Forces," *Military Thought* 17, no. 2 (2008): 89–95.
[570] Col S I Baylev and Col I N Dylevsky, "The Russian Armed Forces in the Information Environment: Principles, Rules, and Confidence-Building Measures," n.d., 12–13; Giles, "Russia's 'New' Tools for Confronting the West," 25–27.
[571] Franke, "War by Non-Military Means," 14–15.
[572] Giles, "Russia's 'New' Tools for Confronting the West," 27.
[573] Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 16.

they are viewed in aggregate across the spectrum of activities that grand-strategy emerges. Considering the Russian methodology and its Soviet precursor, this does not seem accidental; this is an application of reflexive control to strategic scale, and is possibly meant to appear non-malicious or incoherent on cursory inspection.

Network operations are difficult to untangle from the wide breadth of information operations. Military officers Kuznetsov, Donskov and Nikitin directly tackled this distinction, by indicating that "…cyberspace is a component and tangible framework of another, and more extensive, space commonly known as information environment[574]". As such, MONOs are subordinate to grand strategy and thoroughly woven into the larger power dynamic. This is similarly reflected in those who carry them out. The Russian Federal Security Service (FSB), Foreign Intelligence Service (SVR) and Russian Military Intelligence (GRU) have all proven to be prolific network operators. Over the last decade, these agencies and others have engaged in a wide variety of international information activity to include benign reconnaissance, intelligence collection, political and personal active measures, and direct sabotage of information systems and even critical infrastructure.

When examining specific event and presence-based activities, it becomes easier to chart the Russian potential for integrating offensive network operations into warfighting. As the following analysis will indicate, most of the building blocks required to achieve desired effects already exist, contributing invaluable operational experience. Were Russian military forces to similarly invest in permeating network operations through their order of battle as they have with electronic warfare, it would likely prove highly advantageous.

Applied Strategy

Modern Russia aggressively pursues its geopolitical agenda. Regionally and globally, it asserts its interests through means both overt and covert. Its presumptive subservience to a monopolar Western order is no longer applicable; Russia is eager to contend over resources, land, and strategic advantages. Yet this eagerness should not be immediately interpreted as an offensive slant. Russian military thought insists upon a clear and present geopolitical danger from an encircling NATO, bent on its eventual destruction[575]. The key motivation appears to therefore be fuelled by a highly developed – perhaps overdeveloped – threat perception.

Geopolitical concern is accompanied by a realisation that the Russian armed forces cannot currently contend symmetrically with its NATO adversaries, at least not if those are fully committed to conflict[576]. As its conventional military still lags in capacity, Russia seeks to leverage all advantages available to it in order to either accomplish strategic objectives without conflict or at least limit it significantly. This includes – as their doctrine states – "the intensification of the role of information

[574] Lt. Gen. V. I. Kuznetsov, Col. Yu. Ye. Donskov, and Lt. Col. O. G. Nikitin, "Cyberspace in Military Operations Today," *Military Thought* 23, no. 1 (2014): 22.
[575] Adamsky, *Cross-Domain Coercion*, 19.
[576] Giles, "Russia's 'New' Tools for Confronting the West," 25.

warfare", including pre-emptively "…in order to achieve political objective without the utilization of military force" [577].

In 2008, separatist sentiment within Georgian South Ossetia and Abkhazia eventually resulted in an invasion by Russian military forces[578]. Lauding the supposed right of self-determination, the concern seemingly stemmed from the notion that pro-Western Georgia directly threatened the ethnic Russian population within the disputed territories[579]. Deeming it an unacceptable encroachment by the Western agenda, Russian forces proceeded to pummel the Georgian military into inevitable submission, both within the separatist territories and along Georgian cities. While there was never any serious doubt that Georgian forces could not withstand a determined Russian onslaught, the campaign exposed a slew of deficiencies in the Russian order of battle. Disorganised forces, mismatched capabilities, lack of joint operational cohesion and an overall strategic inefficiency led to some unnecessary losses – often due to negligence - before victory was achieved[580].

The Georgia campaign spurred substantial reforms within the Russian military[581]. These could broadly be abstracted to three primary approaches; investment in personnel, advancements of capabilities, and changes in doctrine. Between the three and over the span of the decade to follow, the Russian armed forces have made substantive steps towards improving their capacity to respond to threats and deploy offensively and defensively. While many issues still plague their military forces, subsequent campaigns indicate a rapid learning rate alongside a determination to improve. Whether this was motivated yet again by a perception of threat or expansionist desires does not matter within this context; the end results were the same. Russia acknowledged that it must revisit its strategic priorities and migrate away from its classic emphasis on enemy force destruction in favour of more irregular, non-kinetic means of coercion[582].

A key element within Russia's military overhaul was the recognition that their use of information was lacking. While Soviet-era strategies continuously called for consistent pressure against adversary perception, Russian strategy was relatively slow to catch up in the implementation of these principles for the modern, internet era. As information operations continued, operations against the modern conduits of data - the very networks that became instrumental to modern life in the West – lagged noticeably. Indeed, up until the early 21st century, the internet itself was viewed by Russia with suspicion. Late adoption resulted in delayed adaptation[583].

Russia now extensively relies on several strategic approaches conducive to offensive network operations. Among these; a reliance on asymmetry, the indirect approach, and targeting of perceived

---

[577] Russian Federation, "The Military Doctrine of the Russian Federation."
[578] It remains indeterminate how actively this sentiment was actively stoked by Russian influence operations.
[579] Maruyev, "Russia and the U.S.A in Confrontation: Military and Political Aspects," 11.
[580] Snegovaya, "Putin's Information Warfare in Ukraine," 9–10.
[581] Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare," *The RUSI Journal* 160, no. 4 (July 4, 2015): 40.
[582] Thornton, 42.
[583] Giles, "Russia's 'New' Tools for Confronting the West," 28.

centres of gravity[584]. These previously discussed principles have not only retained their Soviet usefulness but saw new life breathed into them in the information era. Fuelled by wariness of NATO and emboldened by the lack of repercussions to aggressive campaigns against Estonia, Georgia and Ukraine, Russian strategists increasingly deployed more aggressive network attacks against their adversaries[585]. Repeat experiences in different environments globally allowed Russian network operators to accumulate priceless experience in both event and presence-based operations.

The Russian approach to network conflict is the embodiment of the indirect approach. Far more so than its Western equivalents using such capabilities to operationally bypass defences, Russia seeks to employ network attacks across its entire spectrum of conflict to subvert and diminish an enemy[586]. Tactically, network attacks are used to support and augment kinetic effects. Operationally, they are employed to elicit reflexive control in various regions. Most importantly, network operations are strategically used to altogether obviate conventional conflict and coerce adversaries into acquiescence[587].

A relevant analogy can be found in the spread-spectrum communication technique. Its principle is straightforward; rather than transmit across a narrow frequency band, one chooses to transmit the same energy output across a wider range of frequencies. As a result, power output is more diffused, resulting in a transmission that is less observable to eavesdroppers, more resistant to interference, and more resilient overall. The recipient can then reconstruct the original communication by correlating the received transmissions across all frequencies. This technique is now a mainstay in numerous modern platforms.

The Russian strategic approach to network operations is similar. Individual MONOs are not meant to be decisive. Instead, they rely on the indirect approach to target adversary centres of gravity in barrages of low-yield attrition attacks. Rather than attacking a single target with a high-impact effect, operations are carried out frequently and across a swathe of dispersed globally targets[588]. This is done in cognisance of the symmetric limitations of conventional conflict that yet plague their military forces, and the resulting aversion to direct confrontation. The spread-spectrum approach to offensive network activities presents a useful way to integrate such capabilities into military doctrine.

This approach also emphasises the Russian perception that information is a crucial conduit towards attacking modern centres of gravity – the collective will of the people to resist. Considering the Soviet mentality viewing modern Western democracies as socially fractured and incapable of sustained resistance to strife, applying consistent, diffused coercive pressure against these weak points could erode the adversary's capacity to put up a meaningful defence. Clausewitz once discussed applying destructive coercion up to where the enemy's will shatters[589]; the Russian approach applies

---

[584] See chapter 4 for the analysis on strategic principals within cyber-warfare.
[585] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare" (Arlington, VA: CNA, March 24, 2017), 27.
[586] Adamsky, *Cross-Domain Coercion*, 23–24.
[587] Jānis Bērziņš, "Russian New Generation Warfare Is Not Hybrid Warfare," in *The War in Ukraine: Lessons for Europe*, ed. Artis Pabriks and Andis Kudors (Rīga: The Centre for East European Policy Studies : University of Latvia Press, 2015), 45.
[588] Thornton, "The Changing Nature of Modern Warfare," 42–43.
[589] Clausewitz, *On War*, 1:36.

much of this principle and upgrades it to eroding civilian will rather than that of the adversary's military.

Deception also plays a significant role in Russian network operations. Although its quality varies markedly between operations, there is a significant reliance on *maskirovka* – the Russian doctrinal equivalent of deception – in all information operations, offensive or otherwise[590]. Imperative to achieving reflexive control in which adversary actions are seemingly organic rather than coerced, it is understandable why deception plays a key role. The spread-spectrum approach to stringing together a mass of network operations can appear as virtual chaff, making true intent and extent of effects. Occlusion of the operational magnitude leaves adversaries affected yet often not wholly aware of the true extent of Russian strategic intent, manoeuvres and wider political goals.

It does not follow that the Russian approach is entirely optimal. Examining the strategic principles outlined in the previous chapter, several noticeably lack. Among those is the absence of surprise, a comparative dearth of agility, and unsustainably high collateral damage. When these deficiencies accrue, Russia's apparent potency in cyberspace is somewhat diminished. The Russian approach to information operations may shine when unnoticed and against adversaries it has not engaged in active hostilities, but may prove lacklustre against a determined, defensively inclined, actively engaged enemy.

The use of surprise is not mandated for all forms of network warfare, but it can augment its effects. An adversary unaware of an intrusion against its critical networks may find itself the victim of a highly impactful presence-based attack. Instead, Russian threat groups and their corresponding offensive infrastructure are frequently exposed, both as a result of activation of effect and shoddy operational security leading to premature detection[591]. These premature detections reduce the available range of capabilities available to Russia if and when it chooses to commit to active hostilities with its adversaries. Whether this sacrifice is intentional or not, it may impact Russia's odds at being strategically successful in achieving its goals.

Agility is integral towards achieving long-term success. Having the operational capacity to pivot to different challenges, adversaries and circumstances ensures that a force can respond appropriately and win across different theatres. While Russia has made vast strides in modernising its military forces, agility in its network forces remains lacking. Electronic warfare has been thoroughly integrated throughout the Russian order of battle in recognition of a Western reliance on networked command and control to facilitate joint warfare[592]; a similar process must occur for MONOs in order to achieve military success against dispersed enemy networks. Instead, most offensive military activities in cyberspace are still pursued independently by military intelligence (GRU), and intelligence agencies

[590] Franke, "War by Non-Military Means," 24.

[591] Activation entails reaching the effects phase of the operation. This can be seen in their operations against Ukrainian critical infrastructure, against which they have triggered several disruptive and destructive payloads. As for premature detection, Russian operations attributed to GRU, FSB, SVR and other agencies are comparatively exposed with alarming efficiency and consistency. This is in part due to reuse of network infrastructure, malicious code, and offensive techniques.

[592] Grau and Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces*, 289–91.

such as the FSB[593]. These often operate under a wider doctrinal umbrella and pursue multiple concurrent goals, and are thus not always capable of agile responses to crises and combat.

Finally, Russian network attacks often lack the prerequisite finesse. The NotPetya worm – widely attributed to Russian military intelligence[594] - spread to thousands of endpoints worldwide in a blaze of destructive data corruption, yet it was not seemingly intended to do so. Instead, the attack vectors targeting a popular Ukrainian software provider[595] and the geopolitical context suggest that a regional effect was intended. Ending up thoroughly shattering its original operational scope, NotPetya proved to be one of the costliest network attacks in history. Such a brazen attack unduly risks attracting the ire of previously uncommitted parties, either by increasing their support to Russian adversaries or perhaps even directly engaging in countermeasures. Tighter control over MONOs could have resulted in a more localised effect, that subsequently may have sent a more potent coercive signal to the Ukraine. Aggressive collateral impact resulting from poorly developed malicious software appropriating NSA-leaked exploits merely indicates that the Russian threat may not be as severe as they aim to reflect.

Within the Russian spectrum of digital conflict, it is important to delineate between softer information operations and network attacks. While information operations can be crucial to war efforts, they are primarily intended to promote reflexive control rather than be overtly coercive. Similarly, Russian influence, misinformation, and propaganda operations often do not even meet the threshold of an attack. This means that discussing them on equal footing as network attacks risks muddling the crucial distinctions between them.

Russian operations predominantly and consciously skirt the threshold of active warfare. Information operations which are largely non-kinetic are attractive towards such aims, allowing significant operational freedom with relatively little risk and high deniability. Such capabilities can be harnessed both in peace and wartime, and prey upon existing weak points within adversary societies. Russian information operations include fomenting anti-liberal sentiment and conservative nationalism, evoking sectarianism, and undermining the democratic institutions and the agencies set forth to defend them. There is no simple metric for success, as national sentiment and its results are difficult to measure. At the very least, however, it appears that Russian efforts are intended to weaken national resolve and shape the political landscape towards a more pro-Russian, favourable disposition.

To describe Russian operational intensity, it may be useful to observe it as a *diffusion gradient;* the further out an adversary is from Russia's territory, the more dispersed and less overt the measures tend to be. Near-border, former USSR-block nations often receive the brunt of aggressive Russian measures, while Western-European nations are primarily the subject of passive propaganda, disinformation campaigns and intervention in political processes. As such, Georgia, Estonia and

[593] Estonian Foreign Intelligence Service, "International Security and Estonia," 2018, 36–39.
[594] U.S. Press Secretary, "Statement from the Press Secretary."
[595] Maynor et al., "The MeDoc Connection."

Ukraine found themselves on the receiving end of significant Russian offensive measures meant to support concrete strategic goals. Conversely, the United States, United Kingdom, and other Western nations were primarily targeted in measures meant to offset democratic resolve as a whole.

It is mostly within the band of territorial conflict that many of Russia's information operations can actually qualify as attacks, or MONOs. Many of Russia's presence-based capabilities are alternatively used for intelligence collection that is then either weaponised in disinformation campaigns or leaked to damage adversary capabilities. When in early 2018 American researchers revealed a significant compromise of US critical national infrastructure by Russian intruders, they appeared to be within the presence phase of their operations; collecting intelligence and traversing networks to establish capabilities that could then be activated when needed. While such activities are certainly meaningful in Russia's grand-strategy, they are conducted solidly within the remit of peacetime activities against adversaries and therefore worth differentiating from attacks in conflict.

As per the five-step warfare model presented in the first chapter, disinformation activities and aggressive leaks of classified intelligence do not meet the threshold of a warfare-level attack. Such operations often already fail to meet the *impact* criteria but are also primarily not conducted for military-strategic *goals*. As such, these are active tools of political coercion that ebb and flow even outside the context of conflict, though they may intensify as hostilities flare. Presence-based attacks against critical infrastructure such as the numerous MONOs against Ukraine are far murkier to assess and worth inspecting in full. Similarly, high-impact attacks such as NotPetya are important to explore, as they embody the dangers of using an event-based capability within a presence-based operation.

Event-Based Capabilities

Russia is arguably the most publicly prolific nation-state deployer of event-based capabilities. The sheer number of widely attributable offensive incidents between ostensibly Russian elements and adversary nations is unparalleled. Much like Russia's wider predilection towards relying on mercenary and sub-national operators to achieve its military-strategic goals[596], many of Russia's event-based attacks rely on both knowing and unknowing intermediaries. This in turn exemplifies one of the core ideas of event-based capabilities as previously discussed – they must be robust, scalable, and intuitive to use by various threat actors and for different activity types.

In mid-2007, NATO had yet to seriously address the threat from offensive network operations. With a relatively subdued Russian threat and major counterinsurgency operations in rural Afghanistan, the risk seemed comparatively low. For Estonia – a relatively fresh inductee into NATO – Russia has consistently been the primary adversary as the democratic Estonian government whittled

[596] For example, this reliance on external operations has resulted in a 2018 mass-casualty incident in Syria, where U.S. forces opened fire and killed an estimated 200 Russian mercenaries deployed to assist Bash al-Assad's forces. See Neil Hauer, "Russia's Mercenary Debacle in Syria," *Foreign Affairs*, February 26, 2018, https://www.foreignaffairs.com/articles/syria/2018-02-26/russias-mercenary-debacle-syria.

down Soviet symbology from its streets[597]. Yet when the government sought to relocate the Bronze Soldier, a statue erected to commemorate Soviet victory in the Second World War, it resulted in an unexpected surge of unrest within the small country. Starting late April 2007, physical protests were accompanied by an in increasingly determined and coordinated offensive cyber campaign against Estonian networks[598].

Attacks came in waves and were aimed at Estonian government websites and internet infrastructure, seeking to cripple the country's global connectivity. Initially, targeting was sporadic and uncoordinated, with the attack vectors limited to basic traffic flooding tools meant to crudely overwhelm remote servers[599]. By May 9th, the campaign has attracted large international botnets capable of generating a far more significant and sustained traffic load. Numerous websites were temporarily inaccessible until the attack fizzled within a few days[600]. The attacks were treated by Estonia and its NATO allies as a serious incident and resulted in the near-immediate establishing of the NATO Cooperative Cyber Defense centre in Tallinn, accelerating a subsequent decade-long process to formulate strategic guidelines on operating in cyberspace[601]. Due to the widespread attribution to the Russian government, the 2007 attacks on Estonia are often controversially hailed as the first observable case of "cyberwar".

The Estonia attacks do not meet a reasonable threshold of warfare. Utilising the 5-step classification model, the attacks forego quality in favour of quantity, but do indeed seek to affect government *targets*. The *impact* of the attacks was relatively marginal and certainly transient, but it did briefly dent the internet-dependent Estonia's access to online banking and commercial services. Attribution of the *attackers* is murky; while the attacks clearly started in a largely undirected fashion, efforts crystalized into a cohesive effort indicative of more meaningful resources. Yet, it is unclear on whether the Russian government's reliance on fomenting public unrest and employing non-government proxies to act on its behalf qualifies this fully as warfare. In the absence of a strong, direct link to government accountability, this incident cannot effectively be responded to under the guise of warfare. The deniability factor firmly underpinning the attacks fits Russian strategy of avoiding direct confrontation and maintain a sub-conflict relationship with its adversaries.

Rather than an indication of Russian cyber-prowess, the 2007 Estonia campaign is endemic of Russia's inability to use network attacks for tangible strategic gain. Observed at a distance, while Russia was operationally successful at marshalling offensive resources, it failed to affect political coercion on the Estonian government and alter their behaviour. The impact of the attacks themselves was minimal. Internationally, the attacks tightened the alliance between Estonia and its Western neighbours, with the political fallout resulting in a more determined NATO emphasis on cyber defence

[597] Eneken Tikk et al., *International Cyber Incidents: Legal Considerations* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010), 15.

[598] Tikk et al., 16.

[599] Tikk et al., 18.

[600] Connell and Vogler, "Russia's Approach to Cyber Warfare," 13.

[601] This process had several key milestones, including the formation of the CCDCOE in Tallinn in 2008, the publishing of the Tallinn Manual in 2013, and the recognition by NATO of cyberspace as a distinct 'domain of operations' in 2016.

and the establishment of a dedicated cyber-defence centre in Tallinn itself. To its neighbours, the attacks cemented the perception of Russia as an increasingly proactive belligerent. As such, it can hardly be called a success.

The Estonia campaign and the 2008 Russo-Georgian war are often viewed in tandem. This is understandable, as both events happened in rapid succession, featured a presumed Russian aggressor, and heavily incorporated disruptive network attacks. At the time, even the Georgian government – in one of its post-war official reports – labelled the attacks levied against it as cyberwar[602]. As Georgia was markedly less advanced that Estonia in its internet infrastructure, a sustained barrage of disruptive attacks against it both had less and more impact, in varying respects.

There is more evidence of a consolidated effort in the Georgian cyber offensive. Early on, the website "stopgeorgia.ru" was leveraged among others to offer attack tools and targeting instructions, meant to coordinate efforts[603]. Contributions to the campaign included the alleged operational support of the Russian Business Network[604], a then-notorious Russian criminal group with indeterminate affiliation to government elements. Attack methodology included a host of low-yield event-based capabilities that were reportedly pre-positioned[605], including denial of service botnets, various common injection techniques and website defacements[606]. The attacks seemed to target government entities, crippled temporarily crippled Georgian internet access, were at least supported by Russian government elements, geared towards supporting the warfighting efforts, and within the context of broader Russo-Georgian hostilities. As such, whether successful or not – the network component of the Georgian conflict does indeed pass the threshold of warfare.

Examining the results, they too seem underwhelming. The information component of the Georgian military campaign was arguably effective at limiting the government's capacity to communicate with its citizenry, perhaps even hampering some efforts at organising a defence[607]. Yet these attacks were peripheral at best to the overall war effort. Comparatively limited exposure to the internet and a minimal capacity for command and control enabled joint warfare meant that the potential for generating operational effects through network attacks was inherently limited. Much like Russia's wider strategy towards Georgia, the cyber component proved lacking, under-considered and mismatching to the adversary.

Arguably the most effective strategic element out of both the Georgian and Estonian campaigns was the vindication that Russia could aggressively operate in the information pace against its adversaries with no notable consequence. Despite determined attribution and regardless of the disproportionality of the attacks, relations between Russia and the West normalised rapidly after the

---

[602] Government of Georgia, "Russian Cyberwar on Georgia," November 10, 2008.

[603] Evgeny Morozov, "How I Became a Soldier in the Georgia-Russia Cyberwar," *Slate*, August 14, 2008, http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.

[604] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace," 12; Government of Georgia, "Russian Cyberwar on Georgia," 6.

[605] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace," 13.

[606] Connell and Vogler, "Russia's Approach to Cyber Warfare," 18.

[607] E Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Forces Quarterly* 74, no. 3 (2014): 107.

Georgian and Estonian campaigns[608]. In part, this was due to Russia's aggressive dominance of the information space, allowing it to portray a relatively unchallenged narrative that contributed to the appearance of a "fair" intervention by Russia. As such, it was more a success of their wider information operations effort than any meaningful success the use of MONOs.

The civil war crippling Syria since 2011 resulted in a vacuum of power that attracted numerous regional and global powers. Embattled Syrian president Bashar al-Assad narrowly avoided defeat thanks to direct military aid provided by Iran, Hezbollah, and Russia[609]. Increasingly fragmented rebel groups were propped by NATO powers, including Turkey and the United States. The Islamic State and several other jihadi groups sought dominance over wide swathes of territory. The combination of uncertainty and numerous entities fighting for conflicting agendas has resulted in numerous bouts of combat. To Russia, this was also an opportunity to field-test new equipment and offensive techniques developed during their modernisation programs[610]. These included several relevant cases of electronic- and perhaps network-warfare that signal Russia's capacity to manoeuvre tactically.

Russian doctrine relies heavily on the employment of electronic warfare to counterbalance conventional deficiencies in offensive armament[611]. This stems from an accurate estimate of Russian asymmetries in respect to their Western adversaries, along an attempt to deny these adversaries their reliance on network-enabled joint warfare. Such capabilities exemplify just how thin the differences may be between electronic warfare and cyber warfare. They both attempt to influence transmitted information on the electromagnetic and virtual levels, respectively.

Reportedly, in early 2017 several British Royal Air Force (RAF) pilots reported encountering attacks against their onboard GPS from ground-based Russian systems[612]. These exploited vulnerabilities in GPS targeting that were designed to defeat the RAF capacity to guide munitions towards Islamic State targets. Yet due to a dearth of details, it is difficult to assess whether the Russian attacks are electromagnetic interference or an actual attack against the RAF aircrafts' processing of GPS data. The former would constitute a well-established electronic-warfare attack vector, the latter is an indication of a mature event-based capability. In any other context, these capabilities could organically be folded into the remit of combat operations.

Event-based attacks against aircraft GPS subsystems is an intuitive way to incorporate MONOs into military operations. It allows pre-packaging of a repeatable capability into a deployable system such as an anti-air battery or electronic warfare vehicle. It does not require any significant technical knowledge from the operators save the requirement that they know when to employ the capability for maximum effect. If the capability generically targets the GPS protocol rather than exploiting a specific

[608] Giles, "Russia's 'New' Tools for Confronting the West," 4.
[609] Walter Russell Mead, "The Return of Geopolitics: The Revenge of the Revisionist Powers," *Foreign Aff.* 93 (2014): 74–75.
[610] This is made eminent by the deployment of numerous state-of-the-art Russian warfighting platforms, including the Sukhoi Su-35 fighter, The S-400 Triumf air defence system, and numerous variants of the T-90 main battle tank.
[611] Chekinov and Bogdanov, "The Nature and Content of a New-Generation War," 20.
[612] Giannangeli, "Russians 'Hacking into' RAF Crews over Syria."

vulnerability in the RAF Typhoon, it could also be conveniently employed against numerous other enemy vehicles and weapons. Tactically, it is a sound investment that may help offset the risk to friendly forces from smart munitions.

A later case in early 2018 involved a coordinated attack against the Russian Hmeimim air base in Syria. Rather unusually, the reportedly jihadi-led attack involved thirteen drones seeking either to detonate kinetically against their targets or drop bombs overhead[613]. The technique itself was hardly unusual; jihadists have been employing makeshift drones in their attacks in the region for several years before the Hmeimim incident. Yet, the commitment of numerous assets and the coordination of the efforts were surprising. Russian air defence managed to successfully counter the attack. Pantsir-S1 air defence batteries reportedly attained kills against seven drones, while the rest were forced to land as a result of a "cyber-attack" against the GPS guidance modules[614].

Commercial GPS modules for drones are widely available, as are various means to jam and misdirect them[615]. In a majority of cases, an actual attack against the module is not necessary. Instead, exploiting the fact that satellite-transmitted GPS signals are weak due to the distance, attackers would simply transmit a stronger competing signal that would then direct the drone to land. While this technically involves the transmission of data atop the analogue electromagnetic layer, it does not constitute an attack against the GPS component itself. Yet, because the compromise occurs due to misfed digital data rather than interference with the electromagnetic signal, it could still be construed as a tactical event-based capability. Alternatively, if the drones were disabled simply because the GPS signal was jammed, that would still count as classic electronic warfare.

Finally, perhaps the most interesting Russian event-based capabilities are their destructive attack tools, with NotPetya in fulfilling an instructive role. In NotPetya, Russian military intelligence (GRU) had operated a joint presence and event-based campaign. A presence-based compromise of the Ukrainian accounting company MEDoc led to the backdoored software being used to launch event-based destructive attacks against a multitude of Ukrainian entities. Both the capabilities and the operations are worth examining in depth.

First, it is important to identify whether NotPetya qualifies as an act of warfare as per the five-step model. With Ukraine as the intended target and numerous global entities suffering significant collateral damage, it is useful to examine these separately. Starting within Ukraine itself, the *targets* were sufficiently varied and impactful as to qualify. The *impact* is straightforward, as the destructive payload wreaked havoc across numerous networks. As the *attackers* have been publicly identified with high confidence as the Russian GRU they certainly meet the appropriate threshold of

---

[613] Ministry of Defense of the Russian Federation, "Head of the Russian General Staff's Office for UAV Development Major General Alexander Novikov Holds Briefing for Domestic and Foreign Reporters : Ministry of Defence of the Russian Federation," Ministry of Defense, January 11, 2018, http://eng.mil.ru/en/news_page/country/more.htm?id=12157872@egNews.

[614] Raf Sanchez, "Russia Uses Missiles and Cyber Warfare to Fight off 'swarm of Drones' Attacking Military Bases in Syria," *The Telegraph*, January 9, 2018, https://www.telegraph.co.uk/news/2018/01/09/russia-fought-swarm-drones-attacking-military-bases-syria/.

[615] The technology has become so abundant as to be made available as a commercial product for use in non-kinetic corporate perimeter defence.

accountability[616]. *Goals* are difficult to assess, but a strategic agenda meant to weaken Ukrainian resolve to Russian advances is likely. Russia has invested considerably in operating asymmetrically and indirectly against Ukraine, inflicting a severe coercive cost while committing comparably limited kinetic resources. The NotPetya campaign can thus be attributed to the wider Russian strategic agenda. Finally, the *relationship* between Russia and Ukraine includes bouts of combat and a forceful occupation of the Ukrainian territory of Crimea. As such and when reviewing all five parameters, The NotPetya offensive network operation decidedly appears to be an element of cyber-warfare.

It is less evident that Russia engaged in warfare against other nations affected collaterally by NotPetya. While the *targets* remain numerous, the *impact* highly significant, and *perpetrators* the same, neither the *goals* nor the contextual *relationship* between the affected parties and Russia merit observing these attacks as warfare. Irrespective of grievous financial harm caused, the adversarial yet non-hostile relationships between Russia and its fellow nations alongside the lack of strategic intent in harming them contributes to the assessment that NotPetya does not qualify as warfare against these countries and entities. Consequently, NotPetya manifests both as warfare and non-warfare depending on the affected party. The global nature of the internet and the ease in which collateral damage is affected mean that similar spillover is likely to recur in future conflict.

Arguably, NotPetya was not strategically useful. While it was immensely impactful globally, sloppy implementation and operational discipline weakened the acuity of the coercive message. NotPetya featured cannibalised protocol exploits, open-source dual-purpose tools and legitimate modules in its arsenal, creating a crude but effective capacity for rapid network propagation[617]. From a targeting perspective, technical analysis suggests that significant effort has gone into limiting the potential propagation of the malware, only to have these limitations broken by lateral movement between organisational networks instead of just within them[618]. The deceptive attempt at labelling the destructive malware as ransomware almost immediately failed, as it was made apparent that the malware writers had no effective capacity to withdraw ransom money sent to them or subsequently unlock encrypted files. Across all operational and strategic parameters, the malware campaign failed to achieve a strategic coercive or deterrent effect.

Russia appears intent on incorporating event-based capabilities into its strategy. Coinciding with major political strife, such attacks were wielded with increasing sophistication in order to increase coercive pressure and attempt to weaken public resolve. Some parameters indeed coincide well with the before-mentioned approach for utilising event-based capabilities; they were used to subvert existing asymmetries and target weaknesses seemingly endemic to liberal democracies with a Western lean. The capabilities were robust and sufficiently generic as to be effectively delegated for use by

[616] See for example U.S. Press Secretary, "Statement from the Press Secretary."
[617] US-CERT, "Petya Ransomware," US-CERT, February 15, 2018, https://www.us-cert.gov/ncas/alerts/TA17-181A.
[618] Andy Greenberg, "Ukrainians Say Petya Ransomware Hides State-Sponsored Attacks," *Wired*, June 28, 2017, https://www.wired.com/story/petya-ransomware-ukraine/.

mobilised external parties, thereby increasing plausible deniability. Yet, the overwhelming majority of event-based attacks failed to achieve their presumed goals.

This is perhaps due to Russia wielding event-based capabilities under circumstances more befitting presence-based operations. Offensive tools meant for limited scope tactical attacks were used en-masse to attempt a strategic effect, falling short at doing so. Crude attempts at deception only hindered efforts at coordinating attacks and targeting, where these are crucial in event-based attacks. Where event-based attacks thrive at potentially having a localised effect, they were improperly deployed as to create cascading collateral damage at an unprecedented scale. The resulting media attention, scrutiny, public attribution, and international backlash proved antithetical to the limited operational goals originally desired. Rather than diffusing the use of event-based capabilities to external parties, tight operational control integrated into military doctrine could have assisted in augmenting the coercive effect of the attacks. A misunderstanding of how these capabilities could be useful severely attenuated their utility.

Presence-Based Capabilities

The combined Russian effort to penetrate networks is pervasive and diverse. Spanning two decades, hundreds of targets and numerous evolving capabilities, several national agencies have committed extensive resources towards the compromise of adversary assets to promote its grand-strategy. As such, ample evidence exists when examining how Russia engages in presence-based operations. Its aggressiveness and willingness to employ offensive network capabilities reveals both several advantages but also key weaknesses. Succeeding in intelligence operations is one matter, successfully weaponising adversary networks to a strategic benefit is markedly another.

Early indications of Russian malicious network activities can be traced as far back as 1996. In those years, operators later traced back to Russian IP addresses were ransacking numerous US networks with abandon. The FBI-led investigation into what they called Moonlight Maze revealed that intruders were performing unabated lateral movements between universities, government institutions, and military networks[619]. The elaborate operation took years to purge and necessitated a large-scale counter-operation codenamed Buckshot Yankee by the US team that spawned it. The Agent.BTZ malware used to facilitate the elaborate intrusion campaign was fairly complex for its time, with artefacts from its code linking it to an evolutionary chain that persists even today with the Turla malware[620]. The operational practices, technical acumen, and the tools themselves used to facilitate the breach all have grown greatly since the early days of the campaign.

Moonlight Maze was perhaps the first indication that Russia was willing and able to compromise adversary military networks. It reflected the alarming interconnectedness of US military networks at

[619] Bob Drogin, "Russians Seem To Be Hacking Into Pentagon / Sensitive Information Taken -- but Nothing Top Secret," *Los Angeles Times*, October 7, 1999, https://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php.

[620] Costin Raiu et al., "Penquin's Moonlit Maze," *Securelist* (blog), April 3, 2017, https://securelist.com/penquins-moonlit-maze/77883/.

the time, lack of awareness and best practices towards ensuring their safety, and the hold Russian intelligence persistently maintained over these networks. Even as network operations were in their infancy, several phases out of the operational lifecycle including the preparation, engagement, and the presence phases were already routinely being carried out by government operatives for a military-strategic agenda. The logical leap separating Moonlight Maze from a presence-based attack was merely the employment of a destructive module that could wipe all infected endpoints, potentially crippling US joint operations capacity.

Other valuable case studies bely the Russian proven record of supporting military operations with network compromise. In 2016, US security firm CrowdStrike reported that a popular Android application used by Ukrainian military personnel to optimise firing times for the Soviet-era D-30 howitzer has been compromised by malware[621]. The application, which assisted in calculating targeting parameters for the artillery, had been bundled with a malicious tool called X-Agent since 2014. The X-Agent malware has been frequently associated with Russian military intelligence (GRU). Public-domain analysis of the malware did not indicate that its operators sought to disrupt the actual calculations, instead gathering targeting intelligence to facilitate subsequent kinetic operations[622]. As before, only a lack of intent prevented the weaponization of the artillery app compromise; a decision to use the malware solely for an intelligence-gathering objective rather than an offensive one was the sole parameter denying it a role as an instrument of network warfare.

Russia has similarly exhibited an evolved capability for operations against cyber-physical networks. Most notable of these perhaps is the sustained activity against the Ukrainian energy grid. As political strife continues and conflict ensues over disputed territory, Russian activity against critical infrastructure has both pervaded and improved in quality over time. The ostensibly Russian "Dragonfly"[623] campaign exposed by security company Symantec in 2014 was a comprehensive espionage operation targeting industrial control system (ICS) networks, stopping short of operating offensively against them[624]. In 2015, a presence-based operation against the Ukrainian energy grid employing the BLACKENERGY 3 malware did not directly target the supervisory equipment itself but rather achieved its effects through an in-depth understanding of the associated networks and by leveraging destructive malware against the adjoining corporate network used to oversee the industrial equipment[625]. Three years of operations by various threat groups within the Russian intelligence community have resulted in accrued expertise, technical capability, operational maturity, and intelligence on the Ukrainian energy grid.

---

[621] CrowdStrike, "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," *CrowdStrike Blog* (blog), December 22, 2016, https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

[622] The extent of evidence pertaining to Russian use of intelligence garnered from this malware is limited and contentious. CrowdStrike initially claimed that the compromised app led to an 80% attrition rate for Ukrainian D-30s. After challenges to these figures that included the Ukrainian ministry of defense (see Ukraine Ministry of Defense, "Інформація Про 'Втрати у ЗС України 80% Гаубиць Д-30' Не Відповідає Дійсності," January 6, 2017, http://www.mil.gov.ua/news/2017/01/06/informacziya-po-vtrati-u-zs-ukraini-80-gaubicz-d-30%E2%80%9D-ne-vidpovidae-dijsnosti/.), CrowdStrike amended their figures to reflect a 15-20% attrition rate. Yet as it stands, it is unclear how much of this is attributable to information gleaned from the app itself.

[623] This campaign and associated malware is also known as HAVEX.

[624] Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers" (Symantec, July 7, 2014).

[625] Dragos, "CRASHOVERRIDE: Threat to the Electric Grid Operations," 9.

All these culminated in the network attacks that temporarily crippled a Ukrainian power substation in December 2016. The CRASHOVERRIDE malware proved to be a modular framework leveraging previously gathered experience to facilitate targeting a variety of established ICS protocols and generate visible, high-impact effects. Among its modules, CRASHOVERRIDE contained a specific module designed to conduct data wipes on industrial control systems, thereby rendering them unusable[626]. It demonstrated the capacity of its Russian operates to successfully complete the four-step lifecycle of a presence-based operation. CRASHOVERRIDE incorporated extensive preparation both in targeting and capability crafting, successful engagement with the target, an extensive presence phase with lateral movement towards the critical network, and an effects phase resulting in the desired degradation of the adversary.

CRASHOVERRIDE supports the perspective positioning the Russians as technically and operationally mature but strategically lacking. The limited, high-visibility use of the malware revealed its existence and capacity to researchers worldwide, far before it was able to achieve any meaningful strategic effect. Where such a presence-based operation could have been leveraged to create cascading failures throughout the Ukrainian energy grid[627], it instead triggered a localised event of limited operational impact. Where it could have resulted in increased coercive pressure or deterrence due to perceived Russian potency in network operations, it instead revealed Russian over-eagerness, and reduced deterrence due to the success of Ukrainian operators in rapidly mitigating the malware's effects. A powerful presence-based operation was wasted on use with little perceptible value. While particularly notable, CRASHORVERRIDE is not the only instance in which a presence-based capability was used sub-optimally.

In 2015, the French television channel TV5Monde was knocked offline for eighteen hours. In an unusually impactful network attack, an entity calling itself the Cyber Caliphate assumed responsibility and began posting cautionary posts via TV5Monde's social media accounts calling French soldiers to leave territories controlled at the time by the Islamic State[628]. Operationally, it was a remarkable presence-based operation which initially succeeded in promoting the public perception that the Islamic State and its supporters can affect networks on a visible scale.

The TV5Monde hack was then scrutinised for details in an attempt to unmask the attackers. Indeed, subsequent efforts by security companies FireEye[629] and Trend Micro[630] revealed technical indicators linking the operational infrastructure used in the TV5Monde attack to that previously associated with the Russian GRU. What was initially a clever deceptive operation against French critical infrastructure meant to weaken its military-strategic resolve to operate in the Middle East

---

[626] Dragos, 16.

[627] Such a feat would be challenging and require multiple concurrent operations across numerous parts of the Ukrainian energy grid.

[628] Sheera Frenkel, "Experts Say Russians May Have Posed As ISIS To Hack French TV Channel," *BuzzFeed*, June 10, 2015, https://www.buzzfeed.com/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t.

[629] Frenkel.

[630] Trend Micro indirectly received technical data from the hack provided by the French National Cyberseurity Agency (ANSSI) which indicated infections by malware associated with APT28, commonly associated with the Russian GRU. See Rik Ferguson, "TV5 Monde, Russia and the CyberCaliphate," *Trend Micro* (blog), June 10, 2015, 5, http://blog.trendmicro.co.uk/tv5-monde-russia-and-the-cybercaliphate/.

instead galvanised it. Similarly, the clumsy attempt at deception cemented the notion that Russian operators lack operational maturity in their attacks. While the French government and its allies have not directly responded to the hack, it undoubtedly further signalled that the Russians are an aggressive adversary worth defending against. Overall, the strategic utility of the hack proved minimal, perhaps even orthogonal to the Russian agenda.

The strategic inclination for deception by way of network attacks is not limited to the TV5Monde hack. As the Winter Olympics in PyeongChang ramped up in early 2018, the organisers found themselves on the receiving end of a well-planned disruptive network attack against their infrastructure. As networks faltered, drones were grounded and the official Olympics website was disabled[631], security companies worldwide scrambled to analyse the available forensic data and produce findings. Security company Intezer quickly pointed out code similarities between the "Olympic Destroyer" malware and previous campaigns conducted by groups affiliated with Chinese intelligence[632]. A second company, McAfee, released a report and press release implying similarity with capabilities previously used by North Korean network intrusion groups. It was soon made clear that neither indicators of attribution were reliable.

Further research into the Winter Olympics attacked revealed that the forensic evidence was likely planted by the attackers as a "false flag" to misdirect investigators. Russian security company Kaspersky claimed confidence that the attackers deliberately sought to impersonate North Korea by falsifying a technical fingerprint associated with North Korean network intrusion operators[633]. Cisco's Talos published additional information claiming similarity between the Olympic Destroyer malware and MONOs previously targeting Ukraine[634]. Yet both were hesitant in attributing the latest attack to Russia, as false flags muddied the ability to determine the origins of the malware with a high degree of confidence.

Even irrespective of the degree of attribution to Russian state involvement, the deceptive campaign failed. Tell-tale signs of purposeful misdirection were discovered within days, rendering the effort inert. Rather than committing to impersonating a single attacker, the malware developers instead borrowed components from several. Those too fell apart under scrutiny, indicating a lack of capacity to fully produce malware convincingly capable of impersonating another.

It is further unclear what the underlying goal was in the Olympic Destroyer campaign. One curious hint emanates from the lack of effect rather than its presence. While disruption did take place, researchers suggested that the destructive capacity of the operation was far greater than executed, indicating that operators were perhaps interested in political messaging more than wanton

---

[631] Nicole Perlroth, "Cyberattack Caused Olympic Opening Ceremony Disruption," *The New York Times*, February 13, 2018, sec. Technology, https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html.

[632] Jay Rosenberg, "2018 Winter Cyber Olympics: Code Similarities with Cyber Attacks in Pyeongchang," *Intezer* (blog), February 12, 2018, https://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/.

[633] GReAT, "The Devil's in the Rich Header," *Kaspersky Securelist* (blog), March 8, 2018, https://securelist.com/the-devils-in-the-rich-header/84348/.

[634] Warren Mercer, Paul Rascagneres, and Matthew Molyett, "Olympic Destroyer Takes Aim At Winter Olympics," *Cisco's Talos Intelligence* (blog), February 12, 2018, http://blog.talosintelligence.com/2018/02/olympic-destroyer.html.

destruction[635]. In such a case, Olympic Destroyer similarly falls short of achieving its stated goals and contributing to the Russian strategic mission.

The underwhelming results of destructive MONOs should be alarming to Russian doctrine shapers. On several occasions including NotPetya, Olympic Destroyer, and TV5Monde, operators came dangerously close to conducting warfare-threshold attacks against several global adversaries. That is a tremendous degree of risk for a comparatively low-value potential. Considering numerous mistakes and lacklustre operational security exhibited in these attacks, they should perhaps be treated with far more care. Proper integration into strategy, tighter oversight, and dedication of requisite technical resources could both help reduce the risks and increase the odds of success for each one of these campaigns.

Finally, it would be irresponsible to discuss Russian MONOs without mentioning the extensive Russian campaign in the runup to the 2016 US presidential elections. The elaborate multi-pronged campaign included numerous moving parts, including a network breach of the Democratic National Convention, several leaks targeting hawkish anti-Russian politicians such as Hillary Clinton and Victoria Nuland, and a large-scale disinformation effort against US public. While the nuances of the campaign are intricate and exceed the scope of this work, there are several key takeaways that are pertinent towards understanding Russian MONOs and their wider approach to information operations.

The first is that the elections campaign definitively demonstrated Russia's willingness to thoroughly violate another nation's sovereignty through network activities. By targeting national elections, Russian decision-makers chose to compromise the core tenet of a democracy, a feat seemingly guaranteeing some form of retaliation. Yet even as it did so, Russia committed to operating at a sub-conflict level, leveraging soft tools and influence operations to achieve its goals rather than directly attacking voting infrastructure itself and altering results. As previously assessed, the elections hack was a significant breach of US sovereignty but ultimately not an act of warfare due to a lack in direct offensive impact, a purely political goal and lack of pre-existing conflictual relationship between the US and Russia.

The second takeaway is that while Russia arguably succeeded strategically[636], it still failed operationally. Deconstruction of its various operations led to high-confidence attribution by both private sector researchers and the US government itself[637]. The operational deception undertaken by the Russians to thwart attribution efforts was of poor quality, falling apart even under minor scrutiny

[635] Perlroth, "Cyberattack Caused Olympic Opening Ceremony Disruption."

[636] This is assuming the stated goal was to facilitate a Trump-led Republican victory in the 2016 elections, as he was perhaps perceived as being more pliable to Russian grand-strategy and less hawkish in its geopolitical disposition.

[637] CrowdStrike, the security company solicited to assist in the investigation and cleanup of the DNC hack, was fairly straightforward in its attribution, see Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee »," June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. The US government publicly decried the Russian government as responsible on numerous official occasions, see for example DHS Press Office, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security."

by journalists[638]. In this sense, it had almost seemed as if the Russians were surprised by their own success; the operations were designed to weaken American resolve en-masse rather than be individually successful in impacting the course of US politics. Perhaps it was the maelstrom of existing American social issues and political grievances that created a fortuitous turn of events in line with Russian desires.

Russian success was arguably overly reliant on luck and circumstance, but it did not need to be so. As before, tighter integration into decision making cycles and a comprehensive doctrine guiding operators in their actions could have muddled investigations, hampered high-confidence attribution, and prevented galvanisation of the US Congress against perceived Russian interventionism. It was once again a significant impedance of Russian information operations in integrating the tactical, operational, and strategic elements.

JOINT OPERATIONS

Russia is one of few nations poised for success in realising the potential of MONOs. An aggressive pursuit of information operations, a willingness to engage in controversial behaviour, a relative lack of discipline in its intelligence agencies, and a storied history of manipulating information and perception all make Russia an incredibly prolific operator. Yet despite having all chances of success and the perception of unstoppable campaigns against the heart of Western interests, it routinely falters in its ability to achieve its goals through network activities.

Russian MONOs fail to achieve what is expected of them primarily in the first and last stages of the operational lifecycles – preparation and effects respectively. In the initial preparation phase, they do well to develop offensive technical capabilities, but then fall short in crafting credible deceptive identities and maintaining operational security for their malware. They similarly dedicate far too few resources for preventing infrastructure reuse that could hamper subsequent adversary attribution efforts. In the final effects phase they often activate their offensive payloads in poor form, resulting in both limited lasting impact, compromise of sensitive capabilities, and even occasionally revealing operational intent. In other cases, a misapplication of force resulted in severe undesired collateral damage, perhaps outstripping the utility of the operation itself. These limitations are a deciding characteristic of both their presence and event-based efforts.

Event-based operations have been surprisingly well-integrated into military-political conflict, yet without contributing sufficiently to the task. Both in the Georgian and Estonian conflicts, event-based attacks against adversaries were occurring daily alongside additional efforts, kinetic and diplomatic. Russian ability to craft, disseminate and facilitate targeting of pre-packaged, resilient event-based attack tools is a positive indication of a capacity to muster forces. Yet these forces were applied in a manner incongruent with Russian strategic aims, contributing minimally to the overall efforts.

---

[638] Lorenzo Franceschi-Bicchierai, "We Spoke to DNC Hacker 'Guccifer 2.0,'" *Motherboard*, June 21, 2016, https://motherboard.vice.com/en_us/article/aek7ea/dnc-hacker-guccifer-20-interview.

However, there is indication of improvement as Russian event-based activities in Syria appear to be more effective and integrative.

Treating event-based MONOs as the Russians have electronic warfare could have yielded far more promising results. As researchers often suggest, Russia has one of the most elaborate, well-crafted and dangerous electronic-warfare capacities globally[639]. This is in part due to thorough integration through its order of battle, including within infantry battalions and other mobile force structures. Considering the numerous characteristic similarities between electronic and network warfare, a comprehensive integration doctrine for the latter similar to the former could result in a far better application of it towards military needs.

Russian presence-based operations have demonstrated a highly evolved capacity against technically complex targets, including those requiring assistance from subject matter experts. Presence-based malware frameworks have proven modular, and capable of exploiting a variety of targets towards achieving high-impact events. Experience in compromising military and critical infrastructure targets spans at least two decades, suggesting a substantial maturity in pursuing such adversaries. As such, Russia is uniquely positioned to be successful.

What Russia lacks is strategic utility. Presence-based operations were often used as a form of hazy political signalling, or at times thinly veiled strategic misdirection. Both resulted in a decidedly underwhelming contribution to Russian interests, instead either consolidating adversary support, providing crucial insight into Russian capabilities, and compromising valuable offensive tools. Increased discipline and congruence with a broader military or even political strategy could have made far better use of these tools for a longer-term impact.

The overall issue with Russian MONOs is their failure to apply core strategic principles. While they do well to target adversary centres of gravity in the form of critical infrastructure, military targets, and even the population itself, they falter on other guiding principles. Deception is often poorly exercised, and often used when either it is subject to immense scrutiny or altogether unnecessary. The indirect approach is often avoided in favour of tangling directly and overtly with well-defended enemy assets. Russian brashness and under-calculated aggressiveness in its MONOs demonstrates low contemplation of conservation of force. The consequence of this approach is a decidedly low success ratio, and a broad failure to strategically offset the existing military asymmetries. Most importantly, Russia's approach to MONOs increased the risk of armed conflict instead of reducing it. Rather than being an effective component of reflexive control, crude attempts at misdirection in the face of aggressive attacks against critical infrastructure is a dangerous misstep that could eventually cross an undesired threshold. Successive attacks that face on consequence increase the onus of response on the affected parties; NATO would eventually be compelled to respond.

---

[639] Grau and Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces*.

Russia would do well to learn from its own history. Soviet information operations are notorious, and while some were more effective than others, the overall blanket of disinformation effectively hid Soviet conventional deficiencies and strained global alliances. From the military angle, a thorough commitment towards integrating electronic warfare resulted in asymmetry-impacting capabilities and a deterrent that persists to this day. Learning from history, committing to the operational lifecycle, and cautiously integrating MONOs into existing doctrine could provide Russia with the tools to uniquely upset an adversary's capability to resist its influence across all phases of conflict.

7. China and The Taiwan Contingency

Overview

The waters of the South and East China Seas teem with geopolitical friction. The seas represent a crucial nexus for maritime international trade, a concentration of valuable natural resources, and a series of land features that – if militarised – can threaten a wide swathe of territory. To the nations straddling this tight space, the seas represent both an unparalleled opportunity for regional influence and an implement of sovereignty. Through centuries of conflict precipitated by both foreign and domestic forces, an uneasy status quo emerged in the latter part of the twentieth century. While many sides to this equilibrium are increasingly tenuous, one of its most explosive aspects is between two nations that were once one. Both the People's Republic of China (PRC) and the Republic of China (ROC, or Taiwan) view themselves as the "true China". Yet where the former seeks eventual reunification, the latter increasingly pulls towards independence.

This trajectory puts both nations at dangerous odds. As the two nations drift further apart, perspectives on eventual resolution focus on a possible military scenario depicting China's eventual attempt to forcefully reclaim Taiwan as its sovereign territory. The probability of such a scenario is neither remote nor improbable; Taiwan appears to gradually distance itself from the notion of peaceful reunification; in 2016, voters in Taiwan gave the Democratic Progressive Party (DPP) its first ever legislature majority. At the same time, an empowered PRC shows increasing signs of regional assertiveness and a keen desire to pursue its goals militarily. Such a conflict would be far-reaching should it take place, and inherently involves numerous regional forces including South Korea, Japan, and perhaps most of all Taiwan's closest ally – the United States.

An amphibious invasion – which would be necessary in order to forcibly reclaim Taiwan - is considered one of the most complex operations to pull off. Such a campaign requires elaborate logistics, effective mobilization of landing forces, and rapid suppression of an entrenched enemy engaged in an existential battle for its own territory. Time works against the attacker. Should an initial landing attempt fail, defenders would have the opportunity to rally, marshal resources to subdue intruders, call upon regional allies to aid, and affect international diplomatic pressure. In this particular instance, a Chinese invasion of Taiwan is surely to trigger the defensive pact the latter has with the United States. This will likely result in rapid deployment of a US carrier strike group to act both as a deterrent from hostilities and a potential mobile strike force should conflict indeed commence. China would therefore have two key goals; subdue Taiwanese forces as rapidly as possible and prevent allies from effectively deploying and contributing to the war effort.

The Chinese People's Liberation Army (PLA) is keenly aware that rapidly subjugating Taiwan is a monumental feat[640]. To achieve it would require Chinese mobilisation on a previously unseen scale. A crucial component of the effort would include overcoming entrenched Taiwanese defenders and either deterring or defeating US interdiction forces. Only complete strategic success can enable this, and as such the PLA is investing heavily in facilitating its potential victory. One notably novel element of this is the 2015 establishment of the Strategic Support Force (SSF), created to "…maintain local advantages in the aerospace, space, cyber, and electromagnetic fields" while also providing "…attack and defense in cyber and electromagnetic spaces[641]." The enigmatic foundation of the non-frontlines SSF was accompanied by the understanding that network warfare must also be conducted by combat deployed troops at all levels[642], thus splitting the responsibility between strategic and operational needs.

This chapter will argue that *China has developed a doctrinally mature approach to conduct effective MONOs, but it lacks crucial operational experience*. The foundation of the SSF, which unifies operational, technical, and electromagnetic expertise from various areas of the PLA, is a recognition of both the high potential value of MONOs and the underlying difficulties in employing them effectively. This is followed by the understanding that even as the PLA rapidly increases its conventional capabilities, it continues to face a daunting challenge from both Taiwan itself and regional US reaction forces. The PLA must therefore lean heavily on strategic principles discussed as enabled by MONOs; attacking via the indirect approach, limiting detrimental asymmetries, achieving operational surprise, and directly targeting centres of gravity.

The chapter opens with a review of Chinese military modernisation and its implication for MONOs. This includes a review of Chinese regional power projection alongside recent structural and doctrinal reform. The chapter then includes two major components; one reviewing how China would seek to overcome Taiwanese entrenched defenders rapidly and efficiently – a momentous challenge under the best of conditions. The latter and final component reviews how China would seek to deter and defeat US involvement in any such conflict, by limiting its capacity to operate while ideally limiting conventional damage to avoid broader, more encompassing engagements that would result in a loss or stalemate. The PLA faces numerous challenges alongside several interesting opportunities, yet it remains unclear whether it is fit to task in meeting them.

The Chinese Civil War was a violent insurrection of the Communist Party against the reigning nationalist Kuomintang party. Spanning more than two decades from 1927, the resulting conflict stretched well into and beyond the Second World War. Fierce fighting devastated the Chinese mainland before Kuomintang forces were largely routed by their Communist adversaries in 1949. Loss of the mainland resulted in a full Kuomintang retreat to the island of Taiwan, where they re-

---

[640] Easton, *The Chinese Invasion Threat*.

[641] Costello, John, "The Strategic Support Force: China's Information Warfare Service," *China Brief* (blog), February 8, 2016, https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/.

[642] Ji-Jen Hwang, "China's Military Reform: The Strategic Support Force, Non-Traditional Warfare, and the Impact on Cross-Strait Security," *Issues & Studies* 53, no. 03 (September 2017): 4.

established a breakaway government optimistically named the Republic of China. With a communist victory now in hand, the mainland re-carved the battered nation in its image, establishing the People's Republic of China.

Both parties claimed – and indeed to a degree continue to claim – that they are the "true China". The contest over legitimacy soon became a linchpin of the Cold War, which unsurprisingly saw a Soviet-backed PRC counterbalanced by a US-backed Taiwan. However, as years progressed and the Chinese mainland recovered, it became clear that Taiwan's stake at recognition grew distant. Eventually, while the US maintained its stalwart alliance with its island ally, it recognized the PRC as China, a significant move reinforcing the mainland's claim on the UN Security Council seat. China and Taiwan continued to co-exist in a state of pervasive friction. The two remain inexorably drawn to each other's spheres of influence as both seek to define a political narrative on their own terms. Tensions between the PRC and the United States similarly flare hot and cold over Taiwan, with the US seeking to retain its influence over a pro-Western strategically-located island.

An assertive US presence in the Pacific saw Taiwan thoroughly enmeshed in an alliance with the US, further straining relations between it and the mainland. This escalated several times to the brink of armed conflict, culminating in the 1996 Third Taiwan Straits Crisis which resulted in two US carrier strike groups responding to the area in response to PLA missile tests, and a subsequent PRC de-escalation by way of concession[643]. It was an educational moment for the PLA; it poignantly internalized that conventional military parity was – at the time - infeasible against the highly coordinated, advanced US military. New approaches had to be developed, and new capabilities attained rapidly.

The bilateral relationship between the PRC and US has ebbed and flowed over the last five decades. Previously seen as a soviet-era adversary, relations gradually warmed as the Chinese economy increased its interdependency with the global market, standing out as a powerful conduit for trade and manufacturing. This is by no means a steady state. The assertive Chinese push towards establishing soft power and advancing its economic interests has been met with suspicion by some, including the US administration under President Donald Trump[644]. At the same time, the relationship with Taiwan has fluctuated between relative warmth and bristling friction. These trends have largely been commensurate with perceived Taiwanese advances towards a fully-fledged independent democratic government, an unacceptable outcome for the mainland's central communist government. The notion of an independent Taiwan is so offensive to China that officials have frequently and pithily claimed that such moves would result in an overwhelmingly assertive response[645].

---

[643] Jan Van Tol et al., "AirSea Battle: A Point-of-Departure Operational Concept" (DTIC Document, 2010), 3, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522258.

[644] Still in progress, as late as July 2018 the Trump administration has levied tariffs against the PRC in an attempt to counteract perceived trade imbalances deemed as detrimental to the US by President Trump.

[645] Michael McDevitt, "The PLA Navy's Antiaccess Role in a Taiwan Contingency," in *The Chinese Navy*, ed. Phillip C. Saunders et al. (Washington DC: Institute for National Strategic Studies, 2011), 204.

The PRC's rapid growth has been accompanied by an expected increase in Chinese political expectations and the will to pursue them. In part, this manifests in moves to project maritime power in the South China Sea through various contentious proceedings, while more forcefully asserting claims to the disputed territories therein. Controversies abound, including claims of sovereignty over the Spratly Islands, The Daiyou islands, a 200-nautical-mile range defined by the PRC as its Economic Exclusion Zone (EEZ), and of course the island of Taiwan itself. Put plainly, China now claims rights to regulate and enforce all maritime traffic within a large swath of the South and East China Seas. The resulting friction has led to several widely covered entanglements with fishing boats, foreign naval vessels and US military aircraft[646].

The latest development is the militarization of reclaimed islands off China's littoral space. In one such example, the PRC paved a 3,000-meter runway, clearly geared towards hosting large military fixed-wing aircraft[647]. Since 2016, military reclamation efforts of contentious islands – in particular the Spratly Islands - have accelerated, including construction of runways, island defences, and listening posts[648]. This ratcheting up of adversarial behaviour has been poorly received by regional actors, perceived as part of a PLA grand-strategy to project power, enable rapid military response and illegitimately enforce claims of regional sovereignty.

These longstanding strategic developments reflect the PRC's *active defence* strategy. As the 2015 Strategic White Paper details at length, the PRC does not actively seek conflict but rather swift superiority in the face of perceived grievance[649]. This grievance can take many forms; a military incident, Taiwanese independence, or overt assertions of dominance on disputed territories. It is therefore perceived as strategically desirable to preposition PLA forces for maximum effective deployment in their potential time of need. Commensurately, the United States has not remained idle in light of these developments. Over the last decade, the Asia-Pacific narrative within the US has undertaken several major revisions to attempt to both contain and accommodate Chinese regional aspirations. These have all been bound together in a strategy previously labelled during the Obama administration as "The Asia-Pacific Rebalance[650]". Since then, the focus had shifted somewhat to the Indo-Pacific region, signalling a shifting tapestry of alliances and geopolitical circumstances.

Evolving to the Information Era

The PLA now fields an increasingly modern and versatile military. Previous notions of focusing on numerical quantity and land-based force mobilizations have largely been cast in favour of securing

[646] These include an incident in which a PLA J-11 fighter buzzed a US P-8A patrol plane, various incidents in which PLA Navy ships rammed or otherwise harassed fishing vessels, and a near collision between a PLA navy warship and the US Missile Destroyer Cowpens in 2014.

[647] Gregory Poling, "New Imagery Release," Asia Maritime Transparency Initiative, September 10, 2015, http://amti.csis.org/new-imagery-release/.

[648] Frances Mangosing, "New Photos Show China Is Nearly Done with Its Militarization of South China Sea," *Inquirer.Net*, February 5, 2018, http://www.inquirer.net/specials/exclusive-china-militarization-south-china-sea.

[649] The State Council Information Office, China's Military Strategy.

[650] Michael Green, Ernest Bower, and Center for Strategic and International Studies, *Asia-Pacific Rebalance 2025: Capabilities, Presence, and Partnerships : An Independent Review of U.S. Defense Strategy in the Asia-Pacific*, 2016.

China's littoral borders, ensuring interests within its Exclusive Economic Zone (EEZ)[651], deterring US regional involvement and potentially enabling coercive unification with Taiwan[652]. This has far reaching implications on the size, nature and manner of PLA force deployment. While the overall personnel capacity is gradually decreasing[653], troop readiness and equipment quality have been rapidly increasing[654]. China has taken great strides to accommodate modern threats by modernising its doctrine, force building approaches, and strategies. Steps undertaken include reorganising PLA command structure and drastically altering resource allocation[655]. China therefore presents a more promising visage of military readiness, but one which has yet to be battle tested.

Observing the last decade of Chinese doctrine strongly suggests an evolution of priorities. Namely, it has gradually been transitioning from the "People's Army" approach towards a more quality-centric, network-aware, joint operations grand strategy that recognises the qualitative advantages of adversaries such as the United States or Taiwan, and appropriately attempts to alleviate any such asymmetries[656]. This observation has been accompanied by the realization that the next conflict is far less likely to be a massive land-based battle[657], but rather a chain of smaller engagements off of mainland China's shores. These relatively recent developments were labelled "Local war under the conditions of informatisation" by PLA strategists[658].

Active defence is a significant component of PLA doctrine[659]. It outlines that the PRC will supposedly never be the initiator of armed conflict, while retaining the right to proactively act against perceived threats should the need to do so arise. This rather murky language is open to interpretation and leaves a measure of leeway to PRC politicians when directing the use of force. A perceived grievance in the form of a bold Taiwanese step towards independence could readily be interpreted as an opening salvo[660], one breaching existing agreements and therefore inviting direct military countermeasures. Even as China's increasingly aggressive manoeuvres in its littoral seas are dismissed as political flexing, it is acknowledged by observers that the PLA continuously strives towards enabling potential unification, with a stated goal of achieving operational readiness by 2020[661].

---

[651] The State Council Information Office, China's Military Strategy.

[652] Larry M. Wortzel, "PLA 'Joint' Operational Contingencies in South Asia, Central Asia, and Korea," in *Beyond The Strait: PLA Missions Other Than Taiwan*, ed. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: Strategic Studies Institute, 2009), 328.

[653] Edward Wong, Jane Perlez, and Chris Buckley, "China Announces Cuts of 300,000 Troops at Military Parade Showing Its Might," The New York Times, February 3, 2015, 000, http://www.nytimes.com/2015/09/03/world/asia/beijing-turns-into-ghost-town-as-it-gears-up-for-military-parade.html.

[654] Wortzel, "PLA Command, Control and Targeting Architectures," 191–93; Vincent Wei-cheng Wang, "The Chinese Military and the" Taiwan Issue": How China Assesses Its Security Environment," *Tamkang Journal of International Affairs* 10, no. 4 (2007): 109.

[655] U.S. DoD, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China" (U.S. Department of Defense, May 15, 2017), 1–2.

[656] Nigel Inkster, "Conflict Foretold: America and China," *Survival* 55, no. 5 (October 2013): 12–20.

[657] At least not initially. In the advanced stages of a Taiwan invasion, combat operations between land forces on both sides are widely indicated as crucial towards China's success.

[658] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats" (Washington, DC: Center for Strategic & International Studies, December 2002).

[659] The State Council Information Office, China's Military Strategy.

[660] This notion is supported by statements from PRC high ranking officials, who publicly remarked on Taiwanese ploys towards independence as reasonable cause for military action. See Taiwan Affairs Office of the State Council, "国台办新闻发布会辑录（2018-05-16） 中共中央台湾工作办公室、国务院台湾事务办公室," May 16, 2018, http://www.gwytb.gov.cn/xwfbh/201805/t20180516_11955430.htm.

[661] Easton, *The Chinese Invasion Threat*, 22.

PLA references to weaponising information are no idle chatter. Chinese forces have been aggressively working to advance joint warfare capabilities alongside the capacity to target those in their adversaries[662]. Similar to the Russians and the United States, the PLA has identified that the synergy of joint operations results in tremendous value to the modern force; they must in turn both catch up to their adversaries[663] while seeking to deny them those same advantages. At the heart of this process was the primacy of information as the medium permeating all warfighting. It is both a massive potential benefit to those who wield it effectively, but can also create crippling dependencies and deep vulnerabilities. In the latest version of its highly influential publication, the official Chinese publication "Science of Military Strategy" reversed the PLA's previous tendency to deny the use of MONOs[664]. Instead, it both acknowledged and embraced MONOs as a potential differentiator in the modern battlefield.

The PLA's new Strategic Support Force represents the crystallisation of its new approach to informatisation. By consolidating aspects of conducting MONOs into a unified entity, the PLA has acknowledged both the significance and the difficulties in pursuing such capabilities. The new order of battle includes among others elements from the First Department (operations), Second Department (intelligence), Third Department (technical reconnaissance), and Fourth Department (electronic countermeasures and radar)[665]. China's approach seems to echo two key trends in their observation of cyber warfare; that information superiority permeates all operational domains[666], and that deployed forces must be capable of pursuing network operations themselves[667]. By seemingly assigning responsibility for operations of strategic worth to the SSF while allowing other forces to conduct tactical MONOs to achieve local goals, they in fact assign responsibilities roughly analogous to the division between event-based operations and presence-based operations respectively. This uniquely positions the PLA as comparatively doctrinally mature force when it comes to the integration MONOs.

China's greatest detriment in conducting MONOs is its lack of experience. This dearth manifests in two complementary aspects and a corollary. The first aspect is a lack of experience in waging combat operations at all, especially as a joint force relying on networked assets. While PLA military exercises increasingly involve joint operations[668], unlike the United States or Russia it has precious little experience in fully engaging a committed adversary. The second aspect is its lack of experience in conducting offensive network operations. While the PLA is a notoriously prolific employer of network espionage operations[669], there is little evidence suggesting it is routinely engaging in attacking networks to promote strategic-political goals. As a corollary to these two points, the PLA has little experience in applying MONOs alongside kinetic combat operations against an adversary. This places

[662] U.S. DoD, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China."
[663] Ian Easton, "Able Archers: Taiwan Defense Strategy in an Age of Precision Strike" (Project 2049 Institute, n.d.), 8.
[664] McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," 4.
[665] Costello, John, "The Strategic Support Force."
[666] Elsa Kania and Costello, John, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (Spring 2018): 105.
[667] Hwang, "China's Military Reform," 8.
[668] U.S. DoD, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," 3.
[669] Examples are abundant, but perhaps the most notorious is that of Unit 61398, unmasked by private US security company Mandiant in 2013. See Mandiant, "APT1 - Exposing One of China's Cyber Espionage Units."

the PLA at a relative disadvantage, as operational maturity is accrued by experience. Practice makes perfect.

By radically altering its approach to information operations without field-testing the process, the PLA lacks visibility into its own faults. Establishing the SSF and assigning information operations to deployed forces is promising, yet it is unclear if they are capable of achieving any of their stated goals or how they intend to do so. The force structure is new, the technologies they will employ are novel, the challenges they face are fresh, and the adversaries are highly capable. To put it mildly, the degree of uncertainty surrounding any Chinese military action is immense. The Taiwan contingency shines a light on the myriad challenges PLA planners and operators are likely to face when attempting to apply MONOs to an intricate scenario where they could be immensely beneficial.

It is nearly impossible to achieve strategic surprise in a Taiwan contingency. All involved routinely prepare for the eventuality, with most of Taiwan's military forces uniformly dedicated towards curtailing it. Project 2049's Ian Easton similarly acknowledged that "China's leaders have good reason to assume their intentions will be discovered by Taipei well in advance of the attack. Strategic deception is viewed by the Chinese military as desirable, but probably not attainable. Tactical deception, on the other hand, is seen as vital[670]". A pre-emptive Chinese "active defence" manoeuvre will likely initiate escalation of hostilities[671]. Notably, such a scenario is likely to be predicated by a perceived grievance inflicted by Taiwan's government. This could be either an overt policy shift towards independence or as a result of a lesser political conflict spiralling out of control. Escalation of hostilities may indeed be limited to political exchanges or sabre-rattling, providing measures to depressurize tensions succeed in doing so. However, should the PRC assess the timing is right to attempt an overt military operation, the PLA will seek to swiftly overwhelm Taiwanese forces before regional US assets have time to mobilize and respond. Subsequently, the overall strategy sought out by the PLA would be to solicit a Taiwanese surrender as swiftly as possible. Delay entails far greater losses, regional unrest, ally mobilization and international pressure. Surprise, albeit difficult, would certainly help delay American intervention and disrupt Taiwanese mobilisation.

The United States' military is widely considered as one of the most highly-networked, technologically advanced and globe-spanning armed forces. Capably trained, battle-hardened and well suited to joint operation of massive firepower at relative accuracy, it is a difficult adversary to face directly and conventionally. As part of its obligations towards world security, safeguarding economic and geo-political interests while honouring commitments to regional alliances, the US maintains one of its heftiest armed presences in the Pacific. This deployment includes fixed assets, mobile platforms and bolstering those operated by friendly forces in the region[672].

---

[670] Easton, *The Chinese Invasion Threat*, 85.

[671] Roger Cliff, "Anti-Access Measures in Chinese Defense Strategy," *Testimony before the US-China Economic and Security Review Commission*, 2011, 3, http://162.140.209.1/sites/default/files/1.27.11Cliff.pdf.

[672] Van Tol et al., "AirSea Battle," 14.

The regional US presence is overseen by the United States Indo-Pacific Fleet Command (INDOPACOM). It in turn strategically directs the various regional components, including some relevant to the contingency; forces in Guam, Japan, South Korea, Taiwan and most critically – the US Seventh Fleet. The various combatants enable a host of varied fire and support roles. These range from the decidedly offensive such as missile cruisers, to superiority missions such as fixed-wing aircraft operating from both carrier and bases, to the deployment of Special Forces. Sea-based assets are complemented by land-based fixed resources, primarily operating out of Japan and South Korea. The largest of these is the Okinawan Kadena Air Base, hosting the US Air Force's 18th Wing alongside other personnel topping 20,000 active members. The aggregation of various US capabilities in the region translates to a sprawling defensive posture spanning multiple locales, available mission types and capabilities. As such, US military concentrations in the region qualitatively outstrip even some of their hosting nations.

US forces operating in the region benefit from an intricate mesh of interconnectedness between the various fielded elements. From tactical units comprised of infantrymen, warplanes, surface combatants and submarines to higher echelons such as forward operating bases, regional commands and continental agencies, all are thoroughly intertwined through the various incarnations and manifestations of the Department of Defense Information Network (DoDIN). The network serves as a compartmentalized, multi-tiered and multi-protocol communication grid tasked with facilitation of all manners of data transfer[673].

There are dozens of military networks of varying roles in constant use by US forces. Some are globe-spanning networks such as the unclassified NIPRnet and the classified SIPRnet, or the top-secret intelligence-sharing JWICS network[674]. Others are specific to the region of operation, such as the Joint Tactical Information Distribution System (JTIDS), used by US forces and their allies for some warfighter communication[675]. Others still are localized to either a single strike group or a limited operational frame, including closed radio groups and dedicated datalinks. The transmission mediums for such networks are as diverse as the networks themselves, ranging from military satellites, commercial satellites, and terrestrial radio to fixed fibre-optic links. The overall interconnectivity of these networks is a convoluted patchwork of connections, constructed piecemeal over the decades to support increased requirements for joint force operations.

Complete destruction of US forces in the region is unlikely and unnecessary. Rather – and this approach is sponsored by PLA doctrine[676] - an optimal solution is an indirect one that inhibits US capability to intervene in a timely manner. This is accomplished through three primary components: (1) degrading US military capability to conduct joint operations effectively; (2) deterring the US from activating assets due to overwhelming odds of casualties; (3) Directly reducing adversary available

[673] U.S. Army, "Army Field Manual 3-38 - Cyber Electromagnetic Activities."
[674] U.S. Army, "Deployed Tactical Network Guidance" (U.S. Army Chief Information Office, May 31, 2012), 2.
[675] Carlo Kopp, "JTIDS/MIDS - Network Centric Warfare Fundamentals," *DefenceTODAY*, n.d.
[676] David Bennett, "An Analysis of the China's Offshore Active Defense and the People's Liberation Army Navy," *Global Security Studies* 1, no. 1 (2010): 129–30, http://globalsecuritystudies.com/Bennett%20China.pdf.

wartime assets. This strategy has been labelled "Anti-Access/Area Denial" (A2AD) in some US official publications[677], as it is clear that the PLA will seek to quickly prevent US from committing forces to the area in any military scenario. As there is currently no conventional military parity between both actors, the PLA has stated it will seek asymmetrical advantages by way of accurate missile capability, anti-satellite weaponry and indeed, cyber-warfare. Each of the above objectives stands to benefit from a pre-prepared well-crafted offensive network capability, arguably a significant symmetry equalizer.

MONOs only partially fit an A2AD approach to defence. On one hand, denying adversary access to a region and freedom of action within it as a result of persistent event-based attacks against its networks is viable. Event-based capabilities are meant to be reusable and are therefore more robust, thereby implying a persistent threat of denial to would be intruders. In contrast, presence-based capabilities entail intruding directly upon adversary networks wherever those may be. Thus, the geographic aspect inherent to A2AD applies less to non-geographic operational capabilities such as presence-based attacks. They may be used de-facto to facilitate area denial of adversary forces, but such attacks do not as neatly conform to a "threat radius" as other A2AD components often do.

Degrading the joint operational capacity of a thoroughly networked adversary entails striking at communication nerve centres. For a modern military force, these are embodied by 'Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance' – or C4ISR- nodes. These are information hubs tasked with coordinating the operation of local military assets, absorbing and disseminating intelligence, conducting mission tasking, locating and designating targets, and redirecting assets as required. While modern warfighters are more than capable of operating alone or within their tactical frame[678], they are surely to be outmatched by even a relatively inferior opponent whose moving parts are working in relative operational harmony. PLA strategy recognizes the immense value embodied by C4ISR as a target[679], specifically one that potentially reduces enemy preparedness when successfully compromised[680].

Offensive network operations offer an enticing alternative towards attaining the objective, provided they are employed effectively. MONOs provide a wide range of options, contrary to the rather straightforward, destructive qualities of kinetic weaponry. Compromising C4ISR for surveillance rather than kinetically attacking it affords unparalleled enemy situation awareness. As command and control nodes concentrate activity of warfighters in the region, the operational intelligence value of compromising them may be crucial to countering enemy deployments and asset distribution. By employing a network operation, a commander can possibly attain battlefield superiority before the first shots are fired. If situational awareness is insufficient to the task, disruptive MONOs also serve as a beneficial option. Whereas forcibly destroying command systems

[677] Cliff, "Anti-Access Measures in Chinese Defense Strategy," 2.

[678] This varies with the unit type, but generally entails operation within a limited mission area. Examples include infantry companies, tank battalions or warplane sorties.

[679] Vinod Anand, "Chinese Concepts and Capabilities of Information Warfare," *Strategic Analysis* 30 (2006): 789; Brian M. Mazanec, "The Art of (Cyber) War," *The Journal of International Security Affairs* 16 (Spring 2009): 6.

[680] McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," 6.

will immediately trigger countermeasures and lead to conflict escalation, MONOs may enable subtle disruption of data pipelines[681].

Overpowering Taiwan

Taiwan as an adversary presents numerous challenges and opportunities for MONOs. On one hand, limited access to military equipment acquisition and a reliance on aging platforms means that the networked attack surface is significant. Persistent use of the same technologies, networks, and systems leaves neighbouring China with plenty of opportunities to both develop presence-based operations and conduct research and development on event-based capabilities. Conversely, that same reality means that in contrast to their American allies, Taiwan's military has physical redundancies and are likely more capable of conducting combat operations even bereft of networked command and control.

Versus the Taiwanese military, stated PLA doctrine would seek to severely degrade anti-air assets, cripple command and control capabilities, disable defensive warfighting assets such as aircraft, ships and missile sites, and decapitate the military and civilian hierarchy. The opening salvo is designed to facilitate follow-up operations and erode the Taiwanese military's capability to resist the more casualty-prone phases. Put simply, a successful opening salvo has the potential to significantly shorten the duration of conflict and reduce PLA losses, both elements defined as highly desirable by PLA leadership. To achieve this, the PLA is investing heavily in methods and capabilities that would increase the potency of the early stages of conflict, including ballistic missiles, amphibious landing hardware, air power, and MONOs.

Some presence-based operations could yield returns prior to open hostilities. Due to the limited size of its defence-industrial complex, Taiwan presents a fairly small supply chain attack surface. Most of the national security research and development programs are spearheaded by the National Chun-Shan Institute of Science and Technology (NCSIST). Considering China's proclivity for targeting adversary defence contractors, it undoubtedly attempts to similarly target the NCSIST. Successful compromise could result in intimate access to Taiwan's indigenous technology, with the added potential benefit of introducing vulnerabilities that could be exploited in conflict time. The notion of bundling malicious software with equipment is not new to China; it has been previously implicated in a variety of supply chain compromises that either include its own hardware or tampering with existing components[682]. Thus, the operational expertise theoretically exists, yet it remains unclear whether China can wield it to impact the Taiwanese defence industry.

A kinetic approach would rely on a mixture of shock operations and massive mobilisation. Extensive literature has been written on the PLA's capacity to effectively render airbases out of

[681] A key advantage of cyber-warfare includes the capacity to attack below the threshold of inflicting damage; subtle manipulate attacks can often be as detrimental to the opponent and far more attainable.

[682] As of mid-2018, these suspicions have resulted in blocking communications giants Huawei and ZTE from entering the US market altogether.

commission[683]. Strike vectors will include a high volume of short-range ballistic missiles (SRBMs), land-attack cruise missiles (LACMs) and air-launched cruise missiles to overwhelm defences and penetrate hardened aircraft shelters, while simultaneously blanketing runway with specialized munitions designed to disable take-off capabilities. This brute-force approach stands to be highly effective against exposed targets, but is one expected by Taiwan's armed forces for decades, which appropriately applied countermeasures. These include several highly resistant sprawling military command centres built into various mountainsides. The mountainous topography of Taiwan allows for effective dispersal of command and control, which in turn cannot easily be knocked out by ballistic missiles or air attacks, conventional or otherwise. Assessments suggest over 2 kiloton of conventional yield in order to breach compounds such as the Hengshan Military Command Centre in the Yuan Mountain[684], a momentous task even for the burgeoning PLA Rocket Force.

MONOs are uniquely advantageous in this instance by subverting physical barriers. Specifically, in order to effectively serve as command and control centres in wartime, hardened complexes must be networked both to warfighting platforms and other installations. As a result, they can be compromised via their datalinks from an external source, or internally by a sympathetic officer infecting internal nodes. Upon successful compromise, the attacks could potentially be crippling and severely degrade Taiwanese defensive coordination. As previously explored, the preparation phase for such presence-based objectives can be pursued in peacetime, as penetrating, manoeuvring, and weaponizing adversary command and control networks may take months or years. During this time, presence-based capabilities may offer incremental benefits by way of gleaned intelligence on Taiwan's order of battle and force disposition.

Presence-based attacks could offer early benefits against Taiwanese integrated air defence systems (IADS). The efforts to defend Taiwan's skies must crucially be subverted early on to enable PLA theatre air operations and protect amphibious landings. Taiwanese air defence platforms include US-made Patriot batteries, indigenous short-range Antelope systems that incorporate US Sidewinder missiles, and indigenous Tien Kung (Sky Bow) systems. As per a 2016 RAND report, while the PLA Air Force is increasingly capable of rapidly subduing its ROC counterpart, air defences potentially present a greater challenge with high attrition rates for attacking PLA aircraft[685]. Presence-based capabilities could temporarily interfere with air defence systems by partially disabling them or otherwise degrading the situational awareness they provide, allowing PLA aircraft and missiles to penetrate and defeat radars and missile batteries. Such an attack could yield a strategic benefit, but also requires significant skill and resources; while China surely has the former it may not yet have the latter. Penetrating secure military networks, remaining covert, and developing intricate offensive tools meant to impact dedicated military hardware is no mean feat. It requires familiarisation with the

[683] Most prominently by bombing runways with special munitions developed to thoroughly crater the tarmac, effectively preventing all takeoff and landing capabilities.

[684] Easton, "Able Archers: Taiwan Defense Strategy in an Age of Precision Strike," 37.

[685] Michael Lostumbo et al., *Air Defense Options for Taiwan: An Assessment of Relative Costs and Operational Benefits*, Research Report, RR-1051-OSD (Santa Monica, California: Rand Corporation, 2016), 20–22.

platforms affected, technical skill to develop exploitation capabilities against them, and operational oversight to avoid exposing the presence-based campaign prematurely.

Beyond the initial phases of the campaign options for MONOs become somewhat more limited against Taiwan's forces. With the desire to shorten the conflict, it is likely that any sensitive military networks within the PLA's grasp were already attacked in the opening phases of combat. While Taiwanese forces may be in disarray and scrambling to wipe clean their affected systems and networks, generating new presence-based attacks might become exponentially more difficult. This does not immediately imply, however, that MONOs cannot assist PLA efforts to attain airborne superiority and forge a path to expeditionary forces to successfully establish beachheads on Taiwanese soil. Furthermore, a body entrusted with metered use of MONOs such as the SSF may choose to reserve some strategic presence-based operations for this phase of the campaign. Overall opportunities for MONOs are plentiful, including affecting Taiwanese systems meant to provide situational awareness. Impacting these could assist incursion forces in surprising entrenched defenders and keeping them in disarray, a prerequisite if the campaign is to succeed. Event-based operations could be activated against pockets of resistance as these are picked off by the PLA, providing cover for kinetic operations and degrading defensive capabilities.

Alternatively, event-based capabilities against Taiwanese military equipment may retain their potency during the course of the conflict. A few observations work in China's benefit in this regard. The first is that Taiwan relies heavily on US-made equipment such as the F-16A/B multirole fighter. As the F-16's in active use with US forces and their Taiwanese versions share technical characteristics, event-based attacks developed against US communication protocols may work well against their Taiwanese counterparts[686]. Second, while Taiwan's modernisation programs continue apace, they are hampered due to political sensitivities often preventing the US from significant sales of high-quality offensive platforms[687]. As a result, Taiwanese forces are limited to updating increasing quantities of aging systems such as the F-16 and the M60 Patton tank. This means that event-based capabilities developed against Taiwanese equipment may retain their potency for an extended time, allowing the PLA to gradually accumulate an arsenal of such options. Lastly, indigenous platforms such as the F-CK IDF fighter aircraft would need to use systems and protocols compatible with their US-made counterparts in order to facilitate joint operations, thereby extending some of the event-based attack surface to them as well.

Directly attacking civilian infrastructure may become an attractive option. While direct-fire resources are embattled with Taiwanese forces and potentially allied US assets, MONOs are purportedly standing by. Uniquely, the possibility for disruption of civilian life is both possible and mentioned in PLA doctrine[688]. As wholly conquering Taiwan militarily is both a lengthy, arduous

[686] See for example the aforementioned Link-16 and its sibling protocol Link-11, which are also used across Taiwanese forces.

[687] Arms trade to Taiwan has fluctuated in correlation to the relationship with the PRC. As of mid-2018, The US Trump administration has signalled its willingness to resume significant arms sale, much to the PRC's chagrin. See Reuters, "China Demands Halt of U.S. Arms Sales to Taiwan," *Reuters*, April 9, 2018, https://www.reuters.com/article/us-taiwan-usa-submarines/china-demands-halt-of-u-s-arms-sales-to-taiwan-idUSKBN1HG1QJ.

[688] McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," 5.

endeavour and prone to invoking deep civil unrest, coercing the government into capitulation is a far more promising scenario. As a corollary, while military forces attempt to cripple Taiwan's self-perceived chances of victory, network forces can begin to erode the public's morale, stamina and wherewithal. As previously presented, network attacks are unlikely to affect coercion on their own; yet coupled with a withering kinetic campaign, they may serve a caustic function against Taiwan's national fortitude.

Perhaps mostly easy to target would be Taiwan's internet infrastructure. This could be done in several ways, including kinetic operations against fibre landing points and satellite communication facilities used by internet service providers. Alternatively, China could fall back to tried and true methods. In April 2010, a sizeable of the global internet's traffic was rerouted through China by provider China Telecom for 15 minutes in a phenomenon called BGP hijacking. The impact included a full redirection of traffic associated with a broad range of networks, including some sensitive – though ostensibly encrypted - Western government networks[689]. While the occurrence was brief and observers are unconvinced that it was intentional due to its technical characteristics, targeted takeovers of global or regional network traffic remains a distinct possibility. Including traffic hijacking attacks against Taiwanese internet providers could help sow confusion and limit the ability of the island to communicate internally and externally.

Attacking Taiwanese civilian infrastructure with MONOs has several potential benefits. These include ambiguity, deniability and diffusion. Ambiguity is the sheer complexity derived from identifying the nature and source of the attack. Whereas a kinetic attack is immediately visible and detectable, a subtle cyber-attack against sewage treatment, electricity manufacture or civilian logistics is far harder to trace. Deniability relates to the attacker plausible distancing himself from the attack, again a feat nearly impossible with a war-time missile strike. While one can argue that deniability isn't required in a state of warfare, a desire to avoid global escalation with perceived war crimes against civilians remains strong. Controversial actions may be blamed on "patriotic hackers" seeking to aid their country in a time of conflict, or even attributed to war-time chaos. Commensurately, one must recall that the CPC ultimately seeks reunification of Taiwan with the mainland, rather than its destruction. Alienating the population of Taiwan will only serve to complicate future attempts to enforce PRC sovereignty over Taiwan. Finally, diffusion is the subtle art of conducting network operations over time. Rather than singularly striking a target, a clever operator can continuously influence systems by ebbing and flowing within a single presence-based intrusion. By mimicking natural system behaviour and periodically injecting interference, an attacker can negatively impact the target over time without being discovered. In contrast, conventional attacks immediately elicit adversary attention if successful, and therefore subtlety is rarely a requirement.

DEFEATING NETWORK CENTRIC WARFARE

[689] Andre Toonk, "Chinese ISP Hijacks the Internet," *BGPMon* (blog), April 8, 2010, https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/.

Due to the unique blend of geopolitical circumstances, China cannot rely on MONOs to persistently keep it below the threshold of warfare[690]. As Taiwan drifts further away from its notional grasp, options towards reclaiming the island grow decidedly few. Yet even if kinetic conflict will eventually be deemed necessary, that does not mean that MONOs have no potential contribution. On the contrary, they may facilitate strategic surprise that otherwise denied to the PLA or assist in whittling down defenders and their capacity to operate as a joint force. Taiwan's military, a force built in the shadow of its Western benefactors, relies on many of the same doctrinal principles and older versions of the same technologies. It is therefore useful to examine how the new Chinese approach to intangible warfare may be used to counter US and Taiwanese advantages in the region.

US C4ISR capabilities includes three main components that bear the brunt of such activity; aerial platforms such as AWACS[691] planes, fixed bases in Japan such as Kadena or Sasesbo and the US Navy's sole command ship in the Pacific, the USS Blue Ridge. All three assets are defended by fighter craft, anti-air batteries, ground detachments and assorted naval vessels. An effective kinetic strike against the unified C4ISR capability is quite possible given enough resources dedicated to the task of overwhelming the defenders, but it is a highly costly endeavour. In Liddell-Hart's terminology, pursuing such an attack would be adopting the direct approach – a dangerous choice in which commanders strike against an enemy's strongest flank. This would inherently result in far greater casualties and increased friction between the PLA and US forces, further decreasing chances of clean de-escalation.

Due to its scenario-centrality, assaulting US C4ISR is worth examining with further specificity. There are several communication layers that all come together to form the complete command network, loosely corresponding to a simplified version of the well-known OSI Seven Layers Model[692] borrowed from computer science. The first meaningful layer is the physical layer, which includes the actual medium through which communication is conducted. The second shall be labelled the data-packet layer, which signifies the passage of a signal encoded piece of digital data from origin to destination. The third layer shall be designated the data-stream layer, defined as continuous communication between two or more nodes. The fourth and final layer is the presentation layer, which entails reflecting communicated data to operators and allowing them to respond accordingly. Each of these layers can be compromised through different attack vectors, culminating in a highly varied attack surface.

For C4ISR systems, the medium is mostly radio-frequency electromagnetic transmissions. In modern times, these are always encrypted and jam-resistant[693] to prevent opportunistic listeners and standard jamming techniques. However, assuming the message has been successfully received and

[690] This is to contrast other threat actors such as Russian intelligence agencies, that often rely on MONOs and other information operations to pre-emptively achieve their strategic-political objectives.

[691] Airborne Warning and Control Systems.

[692] Hubert Zimmerman, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communications* 28, no. 4 (April 1980): 425–32.

[693] Air Land Sea Application Center, "TADIL J: Introduction to Tactical Digital Information Link J and Quick Reference Guide," June 2000.

decrypted by the other side, there is no originator verification in some US protocols[694]. Consequently, there is some vulnerability to spoofing attacks, provided correctly configured, viable equipment is employed.

Several layers of data sharing and situational awareness protocols are used by the various US warfighters, constituting the overall C4ISR image. These include the JTIDS (Joint Tactical Information Distribution System), an encrypted, jam-resistant radio frequency data transfer platform. The system implements the widely-used Link-16 protocol[695] to facilitate both data and tactical communication between various friendly assets operated by the US and its NATO allies[696]. The complete specification for Link-16, including frequencies, message codes and protocol options are freely available online[697]. Provided the PLA has compromised a single valid Link-16 decryptor, completely reconstructing the traffic is fairly intuitive. The lengthy JTIDS project is currently spearheaded by BAE Systems, a well-known British defence company. Of relevance, BAE had been previously breached in 2009 by malicious nation-state actors[698]. The hack reportedly resulted in data exfiltration, including data pertinent to the F-35 Lightning II Joint Strike Fighter program, the costly collaborative efforts geared towards producing the next-generation multirole warplane.

The data-packet layer is easier to influence via an event-based attack. Curiously, the US regularly publishes a full account of its command and control protocols to a highly detailed technical specification, removing the need to reverse-engineer the protocol. Specifically, modern communication between Link-16 endpoints include 'J12.0' messages, defined in the protocol handbook as "Mission Assignment" messages[699]. Put plainly, a hostile participant in the network can potentially re-task warfighters and assign them new targeting information. Even if the human operator identifies a targeting anomaly, tracking friendly warfighters is usually accomplished via the standardized Link-16 and Link-22 protocols, among others. Due to the pervasive need for real-time performance, there are few to no security measures in place to ensure message legitimacy. As the protocol details, each Link-16 active node is expected to continuously report back its position and sensory output[700] to assist in the overall battlefield awareness. As such, a new Link-16 node could easily register on the current network as a command-capable node. Tracking the origin of a network compromise is difficult in the middle of combat operations.

The data-stream layer holds potential for a different variety of MONOs. If a hostile entity has successfully been introduced into an enemy Link-16 or Link-22 network, it can effectively begin to

---

[694] Understanding Voice and Data Link Networking, 2-19.

[695] Hura et al., "Tactical Data Links," 109–10.

[696] Link-16 enabled platforms include the F15/16 strike fighters, guided missile destroyers and AWACS early warning planes, to name a few.

[697] Air Land Sea Application Center, "TADIL J: Introduction to Tactical Digital Information Link J and Quick Reference Guide."

[698] Siobahn Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009, http://www.wsj.com/articles/SB124027491029837401.

[699] ViaSat, "Link-16 Message Card," October 2012, https://www.viasat.com/files/assets/assets/Link16_NPG_Message_Card_100112a.pdf; Air Land Sea Application Center, "TADIL J: Introduction to Tactical Digital Information Link J and Quick Reference Guide," 19–20.

[700] U.S. Navy, "Electronics Technician Volume 03-Communications Systems," July 1997, 144, http://electronicstechnician.tpub.com/14088/css/14088_144.htm.

transmit conflicting messages to all participants and command units. A repeated attempt at overloading the regional Link-16 deployment is equivalent to a battlefield Denial of Service (DoS) attack. The resulting chaos would be difficult to distinguish in the heat of conflict, especially if a wily attacker is both generating a great deal of traffic while simultaneously spoofing its origin.

Finally, compromising the presentation layer, or specifically the terminals used by US forces is the most plausible scenario by way of a presence-based operation. As seen in architecture diagrams, C4ISR nodes are highly networked to support common services offered by DoD networks, including intelligence sharing, data communication and logistical support[701]. As a result, attacker lateral movement towards C4I networks is expected, where a great deal of damage can be done. Once there, a compromised terminal means the attacker can effectively manipulate any message both received and transmitted. Targets can disappear off screen, and fake messages can be cascaded from the system and onto the unsuspecting network. This will inherently complicate attempts to launch missiles, assign targets to friendly assets and simply conduct battlefield assessments.

The critical hardware and software that makes up US deployed electronics is developed by its expansive defence-industrial complex. These are spearheaded by several corporations such as Lockheed Martin, Northrop Grumman and Raytheon, who most often win the lucrative contracts. Examples are plentiful, including the AN/SLQ-32 Electronic Warfare Suite used by multiple naval platforms and developed by Raytheon and the Navy's Distributed Information Operations System, designed by Lockheed Martin to facilitate battlefield situational awareness[702]. Lockheed Martin was too notoriously breached in 2011 by a foreign entity, during which copious amounts of sensitive intellectual property were exfiltrated from their internal networks[703]. While security and awareness have increased, so has the rate and quality of the subsequent attempted attacks on the company's assets[704].

A clear example of the operational attractiveness of an MONOs against a C4ISR node is the US Navy's Aegis Destroyer. The ship class is entrusted with both air-defence and missile-defence roles for naval strike groups. As such, these combatants are fitted with a highly capable combat management environment named the *Aegis Combat System,* or ACS[705]. This is a catchall phrase encompassing the destroyer's radars, targeting and ordnance capabilities. Considering its centrality and the interconnectedness of the Aegis platform, the opportunity and potential advantages of MONOs are abundant.

---

[701] Global Security, "AEGIS Combat System," Global Security, accessed October 2, 2015, http://www.globalsecurity.org/military/systems/ship/systems/aegis.htm.

[702] Lockheed Martin, "Lockheed Martin to Enhance U.S. Navy's C4ISR Capabilities," Naval Today, July 1, 2014, http://navaltoday.com/2014/07/01/lockheed-martin-to-enhance-u-s-navys-c4isr-capabilities/.

[703] Matthew J. Schwarz, "Lockheed Martin Suffers Massive Cyberattack," *Dark Reading* (blog), May 30, 2011, http://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013?

[704] John McHale, "Record Number of Cyber Attacks Hit Lockheed Martin in 2014," Military Embedded Systems, February 18, 2015, http://mil-embedded.com/3499-record-number-of-cyber-attacks-hit-lockheed-martin-in-2014/.

[705] A high-level component architecture of said ACS is freely available online; see for example Global Security, "AEGIS Combat System."

At the heart of the ACS is the AN/SPY-1 radar by Lockheed Martin, which is managed by the Navy's standard AN/UYQ-70 computer terminals[706]. As documentation reveals, modern iterations of the project have taken strides towards Commercial-Off-The-Shelf (COTS) solutions by adopting well-used architectures that would be cheaper to maintain and upgrade[707]. Updating software versions on shipboard components requires a hefty cycle of preliminary testing and preparation, which means that if a vulnerability is discovered in the legacy Solaris operating system variant used aboard the AN/UYQ-70, it could take several long months before it is subsequently patched out. A shift to standardized, commercial products ensures greater availability of documentation, software and hardware samples to the adversary, reducing the level of complexity required to craft a suitable event-based capability. Once developed, these may retain their efficacy for a number of years, and are not likely to be mitigated during conflict time short of turning off the system itself. A successful event or presence-based attack against the Aegis Combat System could disrupt the trust between operator and machine, thereby increasing confusion and decreasing overall combat effectiveness.

In another valuable example, the latest incarnation of the Tomahawk missile (block IV) used by US forces incorporates full-duplex satellite networking[708]. It both transmits telemetry in flight and is fully capable of receiving remote commands, such as retargeting parameters or an abort order. Data communication is facilitated over a network aptly named "Tomahawk Strike Network" (TSN), which reportedly allows "…anybody who has the authority to log-on… [and] take control of the missile"[709]. The granularity of control is significant enough to allow inflight retargeting of the missile, by an operator situated in a wholly different facility than the operator who originally launched the missile. Plans are underway to even further integrate the missile with its surroundings. This will be accomplished by allowing its targeting module to receive sensory output from friendly assets such as UAVs and land radars while also integrating the entire network to work over the aforementioned Link-16 protocol.

Multi-tiered integration of Tomahawks into a software-managed, remotely-controllable environment means the cyber-attack surface is massive. Indeed, provided the PLA successfully compromises a TSN control node, they can effectively neutralize Tomahawks en-route to strike PLA missile bases, thus preventing the US from intervening in the conflict prior to naval craft arrival on the scene. Interference may be subtle; rather than having missiles veer off course or return to their senders, simply increasing their circular error probable (CEP) by a few metres would result in difficult to detect errors. Even if US operators are eventually alerted to a compromise, they will nonetheless be forced to bring the TSN down pending a forensic investigation in order to avoid possible friendly fire

[706] PR Newswire, "Lockheed Martin and DRS Technologies Deliver 4000th AN/UYQ-70 Ship Display System to the U.S. Navy," PR Newswire, May 11, 2012, http://www.prnewswire.com/news-releases/lockheed-martin-and-drs-technologies-deliver-4000th-anuyq-70-ship-display-system-to-the-us-navy-75230862.html.

[707] Global Security, "AEGIS Combat System"; PR Newswire, "Lockheed Martin and DRS Technologies Deliver 4000th AN/UYQ-70 Ship Display System to the U.S. Navy."

[708] U.S. Navy, "The US Navy Fact File: Tomahawk Cruise Missile," US Navy Official Website, accessed October 1, 2015, http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1300&ct=2.

[709] Jane's, "Exploiting The Network For Smarter Weapon Effects" (Jane's International Defence Review, August 2015), 2.

incidents or any further mishandling of launched Tomahawks. For the duration of the conflict, the damage to combat readiness and efficacy will have already been done.

In the final phase of conflict, a more cautious outlook becomes crucial as all parties involved scramble to adapt and return to operational capacity in the wake of conventional strikes and MONOs used against key networked assets. Some networked platforms have likely been sufficiently compromised as to be extricated from their respective operators' trust circles, therefore rendering them ineffective while they are thoroughly scrubbed. Conversely, intensive measures to rapidly restore reliability to critical networks (such as the US NIPRnet[710]) would likely return some operational capacity, with future attacks much harder to execute. US forces routinely practice recovery procedures, reducing the overall operational cycle duration[711]. This will perhaps give the US and Taiwan a slight edge as networked capabilities gradually return, once again enabling the overwhelming force of the US joint warfare apparatus to function as required.

China's strategy entails utilizing critical capabilities in a single, pre-emptive decapitating strike against US and Taiwanese forces. As a corollary, key MONOs against hardened military targets have likely been spent, leaving PRC capability arsenal rather limited, if not altogether eliminated. A different vector of attack – not easily countered – now becomes far more attractive for PLA operators. These would be keyed towards continued degradation of US and Taiwan military forces still active, while physical forces continue their engagement. Key among these are event-based denial attacks, centred around hampering quality of communications between networked components. Several considerations contribute to the likelihood and success probability of such attacks. Firstly, copious amounts of US military traffic are routinely channelled through public transport means[712]. This includes the civilian Internet, commercial satellites and various other multi-use platforms. Even if the transmitted traffic itself is encrypted - which it often is - disruption of the entire channel via a concentrated traffic flooding will cause reduced service for the medium itself, effectively knocking the communicating parties offline. Secondly, denial attacks are feasible even in the absence of persistent network presence, as they can be launched against the medium itself, much like Internet-based Distributed Denial of Service (DDoS) attacks commonly wielded by low-level hacker-activists and cybercriminals against websites. Thirdly, Taiwan presents a relatively limited attack surface, as the small nation has a comparatively diminutive network infrastructure that may be easily overwhelmed by PLA operators. Fourthly, magnification of attack strength is possible even in lieu of substantial infrastructure, by employing "amplification" attacks[713].

---

[710] USCYBERCOM devotes ever-increasing budgets and attention to both safeguarding and recuperating from attacks against critical networks.

[711] U.S. Homeland Security, "Blueprint for a Secure Cyber Future" (U.S. Homeland Security, November 2011), 16.

[712] U.S. Army, "Deployed Tactical Network Guidance," 1; Coile, "WIN-T SATCOM Overview Briefing," 8; Epperson, "Satellite Communications Within the Army's WIN-T Architecture," 9.

[713] Incapsula, "NTP Amplification: DDoS Attack," Incapsula, accessed October 2, 2015, https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html; Matthew Prince, "Deep Inside a DNS Amplification DDoS Attack," CloudFlare, October 30, 2012, https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/.

TOWARDS RAPID RESOLUTION

China must exploit asymmetry in its military operations. Whether it is trying to reclaim Taiwan, deter US freedom of navigation operations, project power across the South and East China Seas, or forcibly claim other disputed islands in its vicinity, conventional strength matters but is insufficient. The region arguably presents the greatest concentration of modern military power in the world, fragmented across numerous stakeholders. As the Taiwan Straits and the adjoining seas represent critical economic interests for all, any conflict waged would ideally be short and decisive. The PLA clearly pursues this direction, by developing a host of capabilities and doctrine to rapidly offset the advantages of its adversaries.

With its expeditious pursuit of modernisation, the PLA has invigorated its doctrine to reflect lessons learned from its global adversaries. Conflicts waged by and against the US prove both the importance of integrated, network-laden operations and the unique attack surface that they afford. MONOs are emerging as one of several asymmetric capabilities that may subvert the advantages of a technological force heavily reliant upon its qualitative superiority. Creating pockets of operational space can mean the difference between swift victory and protracted stalemates, the latter clearly detrimental to Chinese objectives. Doctrinal writings including Unrestricted Warfare[714] but more importantly the Science of Military Strategy[715] do well to reflect the understanding that information shapes the battlefield. Dominance in the information space may permeate into other operational spheres. The establishing of the Strategic Support Force (SSF) has been opaque to external observers, but similarly indicates an understanding that MONO efforts must be consolidated if they are to be done right. Rather than claiming cyberspace as a domain, Chinese doctrine recognises that information operations and MONOs are present in all other facets of warfighting across the conventional domains. It is about exacting value and efficiency rather than codifying combat in networks as a separate entity with its own governing rules. This early maturity may assist China in rapidly integrating MONOs into warfighting.

As with many PLA capabilities, it is unclear how this Chinese maturity extends beyond the theoretical. Creating organisational entities and organising strategic thought is important, but not nearly sufficient to become operationally successful. In contrast to its prime competitor in the region, the United States, China lacks prerequisite experience in conducting MONOs, joint military operations, and amphibious campaigns. Considering the previously discussed complexity of both presence-based and event-based MONOs, it is unclear whether at this point in time they will serve the nascent SSF well if required. However, the PLA benefits from extensive experience in network espionage campaigns including against applicable defence industries and government organisations. This in turn may offer a degree of familiarity which would reduce the overhead in weaponizing these networks against their owners.

---

[714] Liang and Xiangsui, *Unrestricted Warfare*.
[715] 寿晓松, 军事科学院, and 军事战略研究部, *The Science of Military Strategy* (北京: 军事科学出版社, 2013).

Against Taiwan, the PLA would seek to rapidly achieve victory to avoid an extend period of conflict which would inevitably drag allies such as the US into the fray. Campaign objectives mesh well with the potential benefits of MONOs; achieving strategic and tactical surprise, bypassing concentrations of forces, and degrading networked defences along with the capacity to wage joint operations. For the PLA, MONOs may find a natural slot alongside ballistic missiles in limiting the Taiwan's ability to marshal an effective defence before it is too late. Similarly, a measure of ambiguity afforded by MONOs and their ability to afford pin-point targeting may offer value in creating an expanded anti-air, access-denial (A2AD) envelope against interceding US forces. By creating confusion, degraded situational awareness and reducing hard power projection, US carrier groups and land-based assets may only be able to effectively assist Taiwanese defenders when it is too late, or at least too late to prevent initial amphibious landings.

Finally, while the Taiwan Contingency presents a uniquely complex military scenario for the PRC, its principals reverberate through others. Sudden campaigns to overtake territory are commonplace for the PLA, and regional powers have expressed concerns that this strategy approach may be applied towards their own disputes. In an alarming scenario to Japan and its US ally, the PRC has previously threatened to overtake the disputed Senkaku Islands - or Daiyou by their Chinese name – by what they called "a short, sharp war". This portends exactly the type of conflict in which MONOs could increase the fog of war in service of a limited island-hopping campaign against unprepared defenders. Whether the PLA is capable of pulling an elaborate joint campaign such as this remains to be seen, but indications at least suggest that such as the PLA's strategic intent.

8. A Revolution in Cyber Affairs

Overview

Technology advances at an accelerating pace. Where scientific discoveries were once few and far in between, the twentieth century has reduced the turnaround rate for innovation. This trend has accelerated over the twenty-first century, in which products and devices once considered revolutionary may seem dated within five years of their inception. It is therefore understandable to contend that any model offered for operations in and against networks would not stand the test of time; these too would lose their relevance within a few years of their conception. The very agility that is required in those that operate against technology is required by those who write about it.

The characteristics of modern digitization are accelerated by a few key trends that are expected to become prevalent over the coming years. The first is the development of artificial intelligence (AI), software capable of independent problem-solving in a capacity exceeding existing deterministic methods and machine-learning algorithms. The second is tightly linked to the first and entails the meteoric rise in autonomous platforms across their myriad uses. Self-governing systems are becoming increasingly adept at solving complex tasks previously only accessible to humans, which in turn results in more responsibilities and tasks being offset to them. Lastly, an adoption of simulated environments – augmented reality (AR), virtual reality (VR), and mixed reality (MR), are likely to create new forms of communication, congregation, and operation that may deeply impact the interface between man and machine. Each one of these three trends are already seeping into military research and development, and could adversely affect the manner in which networks may be targetable in the coming future. Yet that is not necessarily the case.

This chapter contends that *the underlying characteristics of MONOs will remain viable at least in the short and medium terms*. The nature of intangible warfare will not inherently change with the next iteration of technology, but rather will exasperate even further. Incorporating AI into decision-making at all levels of warfare would further distance the ability of people to grasp its complexities, thereby increasing the value of targeting technology. An increased reliance on autonomous platforms, rich sensory input overlaid on reality, and opaque algorithms assisting in all aspects of warfare ensures that these would become crucial targets. The notion of weaponizing an adversary against itself becomes even more prevalent.

These latest trends in technology do not represent a break from existing themes; they represent the latest cycle of counter-innovation accompanying intangible warfare. The rise of networking has resulted in MONOs, which in turn might eventually breed counter-MONOs in the form of autonomous AI-based defences[716]. Sparks of this already exist; such mechanisms are now purportedly included in

[716] Reviewed later in greater detail, the idea of AI-enabled network defence has already shown to have limited success. This was recently proven by the DARPA-supported "Cyber Grand Challenge", in which multiple AI "Cyber Reasoning Systems" competed against one

various offering by private-sector information security companies. These claim to employ limited implementations of AI in various instances, such as network anomaly detection, malware analysis, and social network analysis. Such solutions rely on the flexibility of modern learning algorithms to enrich existing approaches rather than supplant them; they are not autonomous network defence solutions. Network defence AIs – potentially capable of outpacing human operators – could be countered by AI-supported MONOs capable of higher levels of agility and adaptability within adversary networks. Rather than targeting sensory inputs which would in turn deceive the operators that observe them, it becomes useful to target technology at more abstract levels. Target the data flows that shape perception for AI, which then incorrectly inform their operators and misalign their situational awareness. The idea of shaping human behaviour remains the same, the attack simply distances further from the humans being targeted.

It is important to continuously evaluate the viability of MONOs. As information security practices arguably improve over time, we theoretically expect to generate less software vulnerabilities. As a result, networks should gradually become increasingly resilient and less susceptible to MONOs. While that may eventually be the case, as of 2018, even decades-old techniques continue to be effective against "hardened" targets, and organisations large and small are repeatedly breached. Trends in increased security are countered by others, such as the proliferation of low-cost, low-quality, low-security devices that impact daily life on a greater scale[717]. Even as the rate of by-default network encryption increases[718], individuals increasingly introduce always-on microphones and GPS tracking into their lives, thereby opting in to monitoring that was previously difficult to achieve. Existing approaches to exploiting software may eventually diminish, only to be replaced by logical flaws or the "poisoning" of the algorithms to which we have delegated so much responsibility.

Even as Libicki claimed software vulnerabilities to be a transient feature of computing, others remain unconvinced[719]. Certain categories of software bugs may reduce in prevalence as issues are systematically addressed and development practices improve. Others would remain and are inherently more difficult to stomp out. New types of vulnerabilities would likely be introduced, corresponding to new technologies. Some may be logical in nature rather than directed at breaking code and would instead seek to subvert the algorithms themselves by manipulating their inputs in significant ways.

The trajectory of software vulnerabilities is extrinsic to the success of MONOs; it is the increased human dependency on technology which ensures continued vulnerability. As humanity delegates more functions to increasingly complex autonomous systems, the very ability to detect that something is amiss decreases. Already, the specific decision-making process that guides algorithms such as

---

another in autonomously detecting threats, thwarting attacks, and mitigating vulnerabilities. See Teresa Nicole Brooks, "Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems," *ArXiv:1702.06162 [Cs]*, February 20, 2017, http://arxiv.org/abs/1702.06162.

[717] Commonly called the "internet of things" (IoT), this refers to the explosive rise of so-called smart devices, ranging from previously simple house appliances to door locks, thermostats and many others.

[718] Adrienne Porter Felt et al., "Measuring HTTPS Adoption on the Web," in *26th USENIX Security Symposium*, 2017, 1326–29.

[719] Libicki, "Why Cyber Will Not and Should Not HAve Its Grand Strategist," 31.

neural networks is fully opaque to all but a handful of people. The sophistication of software logic is rapidly deepening, rendering its rationale hazier to users and even many developers. It becomes therefore plausible that at some point, errors maliciously introduced into these processes may become unnoticeable by people. By one way or another MONOs will likely remain possible for the foreseeable future.

Despite rapid progress, humanity is only at the early stages of autonomous software and is hence limited in its capacity to assess its impact. This is no less true for the viability of MONOs, though some key indicators are already emerging. Militaries are already introducing growing quantities of autonomous platforms across all levels of operations. These platforms will be more capable of performing complex tasks. Use of artificial intelligence may enable battlefield superiority in a networked world, but at a cost; human ability to comprehend and directly control the elements of warfare may shrink, increasing the threat and potential efficacy of MONOs as an operational method of choice. If more aspects of warfighting are governed by software and software-controlled hardware, the software itself becomes a key target worth relentlessly pursuing, either through event-based or longer presence-based capabilities.

This final chapter is understandably more limited than its formers. For one, access to details on bleeding edge military developments mentioned throughout is understandably restricted. Still, strategic publications indicate overall directions and developmental priorities. Similarly, developments within the military sector are often tightly correlated to advancements in the private sector, those being less opaque. At the same time and with the accelerating pace of technological advancements, even trends may shift or be rendered obsolete within a relatively limited timespan[720]. As previously detailed, advancements form counter-innovation cycles that may be difficult to predict. Each cycle is reflective of the previous step, which makes predicting beyond a single cycle unwieldy. Yet, even modern advancements in networking, robotics, multi-domain warfighting, and artificial intelligence have all been discussed extensively since the twentieth century. As previously indicated in the chapter on intangible warfare, technological developments and their integration into warfighting are firmly rooted in history. While the pace of advancement may accelerate, its products have a traceable lineage to existing developments. The challenges of tomorrow may be different, but they will undoubtedly evolve from todays.

Becoming Less Vulnerable

It is a point of contention whether software is becoming more secure overall. If exploitable software vulnerabilities are on the decline, network operations against secure environments become significantly harder to accomplish without an immense investment of resources. Were this to be true, the economy of MONOs would alter to where resource cost appears less inviting, deterring decision-makers from risking remaining capabilities within the arsenal. Opinions on the direction of overall

[720] Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," *ArXiv:1802.07228*, February 2018, 58–59.

vulnerability of software run the gamut and include perspectives both grim and optimistic. In reality, both sides offer merit in the arguments. It is reasonable to simultaneously claim that security practices have dramatically improved over the last two decades while acknowledging that the attack surface has remained massive, and in some cases expanded significantly. We are safer in some respects and more exposed in others. This is true both for the military use-case and the civilian.

On the positive, major operating systems now enjoy significant security features rendering compromise increasingly difficult. This extends to up-to-date versions of Microsoft Windows, but also improvements to the various Linux/Unix implementations frequently also used in servers and hardware deployed in military equipment. These improvements are accompanied by streamlined patching cycles that mitigate risks faster than previously possible, further degrading the long-term viability of a given attack vector. Additional, security-centric operating systems have been publicly available for several years, offering a tight controls and compartmentalisation of sensitive environments, limiting the overall impact of compromising specific software[721]. Even as mobile devices proliferated, they have become increasingly resistant to compromise. Technology company Apple has enshrined security as one of its key tenets, and its signature hardware and software environments are often favoured by security researchers for their more limited attack surface.

Security mitigations applied across all levels of computing have made achieving full system compromise trickier. Success may now require complex exploit-chaining[722], raising the cost of success against capable defenders. Perhaps the biggest evidence of this may be seen in the booming exploit market, in which private companies seeking to purchase exploits offer rapidly increasing pay-outs[723]. Exploits against high-value targets are more expensive both because of increased demand but also due to a declining supply. The entry price has therefore increased to levels that may deter some under-resourced militaries from effectively participating.

In sharp contrast, even ancient techniques have retained their operational utility. The underlying model of network operations has not changed, despite best efforts by network defenders to reduce its effectiveness. Perhaps most pertinently to the military domain, frequently updating vulnerable hardware and software remains a key challenge in maintaining an operational environment relatively resistant to MONOs. The need for extensive testing, associated costs, risks of decommissioning equipment for upgrades, and the continuous need for interoperability with legacy equipment means that upgrades may be few and far in between. In some cases, recently detected vulnerabilities were embedded so deep in the hardware stack that only radical patching of core functionality could mitigate the vulnerability[724]. In other cases, military equipment developed opaquely by contracted providers is

[721] Examples include Qubes, a fully open-source secure Linux variant pertaining to compartmentalise running processes, and Trusted End Node Security (TENS), A US Department of Defense lightweight Linux variant.

[722] This process entails capitalising on multiple vulnerabilities within the targeted system in order to gain administrative access and achieve persistence. At times, the original exploit used to gain foothold is insufficient to the task and requires lateral movement within the system itself through privilege escalation exploits.

[723] For example, as of mid-2018, private exploit company Zerodium offers 1.5 million dollars for a remotely executable exploit requiring no user interaction for Apple mobile devices. See https://zerodium.com/program.html.

[724] See for example the Spectre and Meltdown CPU vulnerabilities, which led to widespread panic as they were originally deemed unpatchable. While the vulnerabilities were eventually addressed via manufacturer patches and operating system kernel fixes, it indicated

not subjected to the same levels of public scrutiny and may therefore exhibit flawed secure development processes. Considering the exponentially increased intricacy of a single unit of military hardware, the vulnerable attack surface has possibly grown faster than commensurate mitigation efforts[725].

Vulnerabilities are not inherently about software. As often repeated, the most vulnerable element in many circumstances is the people within them. While the argument on the prevalence of exploitable software bugs is certainly relevant, humans retain their innate vulnerability to compromise. The evidence to this is damning; even low-quality phishing still succeeds at scale, including against high-value targets[726]. Many successful network operations were in some part facilitated either knowingly or unwittingly by a compromised individual. This reality is not likely to change in the foreseeable future. Perhaps even the opposite is true; people would become even more vulnerable as software gradually becomes less so.

Humanity has gradually introduced vulnerability into its own circumstance. One anecdote that demonstrates this is the story of Strava. A seemingly benign private-sector company developing fitness devices that track user performance found itself engulfed in an inferno of global attention from security researchers after it unveiled an interactive map in late 2017[727]. The map – intended to be an attractive visualization of Strava's market penetration - aggregated anonymized user activity into heat maps, showing where its fitness trackers were used. As many observers quickly realized, the map inadvertently revealed patrol routes within military bases, sensitive facilities, and foreign deployments of forces[728]. It was also possible to deanonymize users with relatively minor effort. There was no software vulnerability involved with this incident, but it had shown how even military forces could be threatened by improper use of civilian technologies by its members. It demonstrated a radical expansion of the threat model previously only minimally considered.

Strava was not an isolated incident; individuals and groups blindly give themselves to technology. For perceived benefits people relinquish privacy, sensitive data, or control over aspects of their lives. As people increasingly intertwine their daily routine with more connected devices, they further increase their vulnerability. These devices become increasingly significant in shaping perception of reality itself; tampering with them and the data they rely on may therefore alter that perception in weaponizable ways. Military forces are no different in this respect, a growing reliance on data feeds and technology makes users inherently more dependent, and therefore – vulnerable.

---

how complex mitigation was for some hardware vulnerabilities. See CERT.org, "CPU Hardware Vulnerable to Side-Channel Attacks," Carnegie Mellon University CERT, January 3, 2018, https://www.kb.cert.org/vuls/id/584653.

[725] One apt anecdotes describes the exponential increase in code complexity deployed within military aircraft. See Robert N. Charette, "This Car Runs on Code," IEEE Spectrum: Technology, Engineering, and Science News, February 1, 2009, https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code.

[726] Verizon, "2018 Data Breach Investigations Report" (Verizon, 2018), 8, https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

[727] Drew Robb, "Building the Global Heatmap," *Strava Engineering* (blog), November 1, 2017, https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de.

[728] Jeremy Hsu, "The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data," *Wired*, January 30, 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

One such example of this is the increased use of augmented reality (AR). AR includes technology that overlays what the eyes normally see with contextual information. Versions of this have existed in militaries for many years – heads-up displays for aircraft that overlay targeting information and telemetry are long operational. As the technology matures and becomes more prevalent in military use, it becomes a vulnerability in its own right. Relying on augmented displays rather than physical perception can create a dependency which could be exploited through MONOs that seek to shape what the operator sees, causing undesired behaviour. With some MONOs already seeking to softly impact the overall perception of reality, this trend may gradually increase in prominence.

On Intelligence

As with countless other concepts, artificial intelligence (AI) lacks a consensual definition. Even as it explodes in popularity and brandished in corporate marketing campaigns, the boundaries of where an algorithm ends and artificial intelligence begins are blurry. Per Horowitz, one largely agreeable component of AI is that it is capable of achieving its goals in a broader range of circumstances and environments than traditional algorithms[729]. Others designate AI by being able to solve tasks of sheer complexity normally handled only by humans, such as speech analysis and contextual decision-making[730]. The underlying approach to solving tasks more organically mimics human behaviour by gradually adapting and learning from experiences both failed and successful[731]. AI is thus an approximation of facets of human intelligence by software patterns adapted to improve with further exposure to inputs.

It is important to distinguish between two primary forms of AI. Limited applications are already at play in various capacities as *narrow* or *modular artificial intelligence*, capable of solving domain-specific tasks. These systems may exhibit above-human levels of success at environments with limited variables and rules but cannot be broadly applied against any domain without significant adaptation. Examples of this include the "Deep Blue" system that defeated Garry Kasparov at chess in 1997[732], or the systems competing in DARPA's Grand Cyber Challenge[733]. Such systems may achieve previously unseen performance when set to specific tasks but would otherwise not be immediately useful to solving others. The other type refers to *artificial general intelligence (AGI)*, capable of assessing and resolving challenges across any number of domains by intaking environmental data and generating a favourable behaviour. Such systems are infinitely harder to create and would represent a substantial leap in the field if successfully developed, though they form the original crux of AI research[734]. AGI is

[729] Michael C Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018): 40.

[730] M L Cummings, "Artificial Intelligence and the Future of Warfare" (Chatham House, January 2017), 2.

[731] Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," *Journal of Strategic Studies* 39, no. 5–6 (September 18, 2016): 794.

[732] Deep Blue was an IBM supercomputer purpose-built to excel at chess. For a detailed analysis of the system and its development, see Murray Campbell, A Joseph Hoane Jr, and Feng-hsiung Hsu, "Deep Blue," *Artificial Intelligence* 134, no. 1–2 (2002): 57–83.

[733] Brooks, "Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems," 8.

[734] Ben Goertzel and Cassio Pennachin, eds., *Artificial General Intelligence*, Cognitive Technologies (Berlin ; New York: Springer, 2007), 15.

viewed with apprehension by many who are concerned with the unpredictability of an entity capable of rapid self-evolution beyond human control or understanding[735].

The overall appeal in AI – even narrow AI - is understandable and extends far beyond military applications. Autonomous vehicles capable of responding responsibly to their surroundings promise a revolution in transportation. It may assist individuals in making responsible choices daily by more objectively assessing data and achieving bias-free optimal decisions. At higher levels, AI may contribute to running increasingly complex networks such as so-called smart cities. This includes automated allocation of resources as they are needed, rapid detection and mitigation of faults, and aggregated feedback to operators who can then action as necessary. The motivation to adopt AI for numerous uses is mounting, and its integration into the security domain will likely be correlated with its overall adoption by society at large[736].

Artificial intelligence is already being considered for numerous military applications. The People's Republic of China invests heavily in a spectrum of AI developments in an attempt to ensure long-term technological superiority over its global competitors[737]. The United States has similarly identified AI as significant to its technology-led "Third Offset" strategy first penned in 2014, whereas such technologies serve alongside autonomous platforms in cementing US power projection in an increasingly contested geopolitical environment. In a 2016 speech by then Deputy Secretary of Defense Robert Work, he openly stated that "…we believe quite strongly that the technological sauce of the Third Offset is going to be advances in Artificial Intelligence and autonomy[738]." Applications range from the tactical to the strategic, from more capable missile guidance and steering to battlefield planning. Considering their limitations to domain-specific problem solving, AI is not the panacea it seems to be. Much like MONOs, it will only be useful if used correctly. It requires identification of opportunities, generating appropriate datasets, and responsible incorporation of such mechanisms into both new and existing platforms. Perhaps even more so than in other areas, artificial intelligence offers unique opportunities in enabling both event and presence-based offensive network operations. Seeing that MONOs represent the repeat compromise of computers and networks, they enjoy a fairly predictable set of rules and characteristics that would fit narrow AIs. As Horowitz claimed, rather than being the weapon itself "AI is actually the ultimate enabler[739]."

The use of artificial intelligence in strategic decision-making is particularly of note. The allure certainly exists. The modern battlefield is complex and difficult to effectively assess by the human mind, which is both inherently limited in its capacity to process sensory inputs and heavily prone to decisional bias. As such, autonomous platforms capable of objective analysis represent the potential to aspire to an objective strategic optimum. Yet handing matters of strategic consequence to AI risks

[735] The list of those concerned from the potential impact of AGI includes physicist Stephen Hawking and technology industrialist Elon Musk, among others.

[736] Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," 61.

[737] Kania, Elsa, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power" (Center for a New American Security, November 2017).

[738] Robert Work, "Remarks by Deputy Secretary Work on Third Offset Strategy," U.S. Department of Defense, April 28, 2016, https://www.defense.gov/News/Speeches/Speech-View/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/.

[739] Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," 41.

turning them into centres of gravity by their own right; these platforms may eventually become pivotal to command and control thereby becoming worthwhile targets by their own right. Adversarial algorithms meant to specifically pray on weaknesses manifest in such systems already exist, with the field potentially facing a surge of research activity as their importance increases[740].

For presence-based operations, relying on AI may assist decision-making and manoeuvring within adversary networks. By automatically assessing sensory input received from malware infections in adversary networks, viable options may be rapidly generated and actioned upon by operators. The use of such platforms may effectively shorten the presence phase by reducing the need for operator-led lateral movement within networks. Autonomous presence-based operations may also fair better at detecting fault lines within networks and vulnerable endpoints, increasing the chance of success. Alongside with shortened presence, reducing the chance of human error due to AI-led command and control would reduce the risk of detection. As previously explored[741], the presence phase of an operation consists of numerous micro-cycles in which operators manoeuvre implants within compromised networks, retrieve additional information, perform assessments, and decide on follow-up actions. While creativity may be useful, these processes are often repetitive and conform to the same set of circumstances. The laundry list of activities includes maintaining operational security, identifying vulnerabilities and credentials used for further lateral movement, locating key sources of intelligence, and obtaining privileged access to the objective systems. The methods to accomplish these activities is often also repetitive and directly in response to certain telemetry; use a certain vulnerability against a certain type of endpoint, run a certain module to obtain additional data, avoid endpoints where a certain brand of anti-malware solution may be deployed. Consequently, training AI to mimic operator behaviour may not only be possible but a relatively cost-effective way to dramatically scale MONOs. By relegating all but the most complex, hard-to-breach target networks to autonomous network intrusion platforms it may be possible to generate higher-quality effects against a broader set of targets.

For event-based operations, limited-scope artificial intelligence incorporated into weapon systems may increase their robustness. A single platform may be able to; (1) intelligently curate viable targets, (2) enumerate vulnerabilities per target, (3) choose applicable exploits, and (4) choose mission-relevant offensive payloads[742]. This reduces both the overhead and expertise required by deployed operators, which may reduce hesitation by commanders in employing such capabilities. If such a system is able to calculate the probability of success for attempting to compromise an adversary system or network, commanders can more realistically assess whether such an option is viable.

In the preparation phase, AIs may eventually contribute to both presence and event-based MONOs. As vulnerability research is often a significant component in facilitating offensive operations,

---

[740] Examples include the 2014 paper demonstrating fooling classification neural networks, see Christian Szegedy et al., "Intriguing Properties of Neural Networks," *ArXiv:1312.6199 [Cs]*, December 20, 2013, http://arxiv.org/abs/1312.6199.

[741] See Chapter 2: "Offensive Network Operations".

[742] Patents suggesting this course of action have already been approved, though their method of implementation is unclear. See for example Hershey, Chapa, and Umberger, Methods and apparatuses for eliminating a missile threat.

an AI capable of more rapidly and thoroughly dissecting adversary protocols, software, and hardware may prove invaluable. While some automated capabilities already pervade vulnerability research[743], these are more limited in scope and primarily serve in identifying potential bugs meriting additional investigations. As previously mentioned, the vulnerability research process is expensive in both time and resources; even capable entities such as the NSA have only so much top-tier talent to assign to the task. Being able to delegate aspects of this research to artificial intelligence approximating their human counterparts could both broaden the scope of available targets while reserving key talent to unique and novel challenges where human creativity is irreplaceable.

Contribution may not be limited to assisting human operators; it may eventually supplant them. At least initially, some capable nations are seeking to augment network defence with autonomous capabilities that have reaction times and agility outstripping that of a person or group of people. To parse and assess massive quantities of data requires significant computational resources. These quantities grow as sensors improve and proliferate, a distinct characteristic of both the modern battlefield and modern networking in general. DARPA invests in many such projects, ranging from anomaly detection, improving the resilience of networks to attack, and automatic patching of vulnerabilities[744]. The innovation cycle that had bred network operations will eventually result in AI-enabled network defence as a counter-innovation.

Innovative network defence solutions would require innovative MONOs. As operators become insufficiently dynamic as to overcome automated network defences, the business case for autonomous offensive capabilities may evolve organically. Beyond just facilitating rapid lateral movement, offensive platforms would need to make intelligent decisions and respond to high-tempo changes made in networks by deployed defences. This eventual maturation of MONOs into autonomy offers advantages but also considerable risk; it becomes difficult to detect the point in which operators and system developers lose effective control. MONOs may become opaque black boxes, which must be trusted to perform as desired behind enemy lines even in highly variable situations. The amount of uncertainty introduced and the necessity to cut the human operator out of the decision-making loop may prove dangerous, as the risk of cascading impact that already characterises MONOs may exponentially increase. Even after two decades of network operations and within manually-controlled operations, capable nations still frequently fail to safeguard their tools and avoid collateral damage[745]. The significance of autonomy in MONOs is therefore an unknown quantity.

Unmanned platforms have been in military service for over two decades. Their classic roles vary but often concentrate either on reconnaissance or as precision weapons. As the underlying technologies matured and proliferated, drones increasingly occupied additional battlefield roles, including communication, electronic warfare, logistical support, transport, and even search and

[743] One such automated method is called *fuzzing*, in which software attempts to automatically find faults in other software by providing it a variety of unexpected inputs in hopes of creating unexpected, exploitable behaviour.

[744] Shen, "The Information Domain and the Future of Conflict."

[745] Many such examples have been mentioned throughout this thesis including internal threats such as Edward Snowden exfiltration of broad NSA data and external threats such as the Shadow Brokers theft of NSA TAO network operation capabilities.

rescue. They come in every size and are deployed across all physical domains; air, land, sea and space[746]. Today's unmanned platforms are more versatile and capable of enabling accurate operations at scale while minimising physical risk. With improvements in robotics and the aforementioned artificial intelligence, this trend is unlikely to reverse in the foreseeable future.

Autonomy in military platforms had become realistic. In addressing the viability of such systems, the question has gradually transformed over the last two decades from "can this be done?" to "how should this be done?" The tide of robotics cannot be prevented, only channelled in directions where it may have higher utility and lower risk; such considerations exceed the scope of this thesis but would become instrumental to modern warfare. For those who assess the potential impact of robotics, concern mounts to alarming levels. The US Army Training and Doctrine command views them as "potential game changers" that "…can provide a decisive edge over an adversary unable to match the capability or equal the capacity[747]." Russian military scholars have repeatedly expressed that robots are due to perform myriad tasks in modern warfare, making them a key characteristic of new-generation warfare[748]. Official Chinese publications view unmanned intelligent platforms as a key reason that the traditional centres of gravity in warfare have been displaced[749]. The consensus seems to be threefold; (1) there will be an exponential increase in the use of autonomous platforms; (2) these platforms will become increasingly capable of performing complex roles, and; (3) they are both a threat and an opportunity to upset existing symmetries.

Increased adoption of unmanned platforms increases a military's exposure to MONOs. Capable as they may be of feats unattainable by human beings, they also incur unique vulnerabilities. Subversion of software used by a human operator may cause undesired results and – in extreme circumstances – even physical harm, but it does not directly target the individual. By their nature as governed by software, unmanned systems are fundamentally exposed to compromise by MONOs either directly or indirectly. As aptly put by Hartmann and Steup in 2013; "[Unmanned Aerial Vehicles] must be classified as highly exposed, multiply linked, complex pieces of hardware[750]." The possibility to inflict complete combatant shutdown as a result of a successful network attack against the system is both real and significant.

The United States was caught by surprise in 2011 when a RQ-170 Sentinel UAV suddenly became unresponsive while conducting a mission within Iran's borders. Iranian media soon announced that they had not only intercepted the drone, but effectively interdicted its directives to force it to safely land on an Iranian airstrip. While the United States had not officially acknowledged the details of the incident, the Obama administration had officially petitioned the Iranian government for the return of the aircraft. Theories of how this came to pass were plentiful, but one likely explanation persisted;

---

[746] One example of an unmanned space vehicle is the Boeing X-37, used by the US Air Force for repeat undetermined missions.

[747] TRADOC, "The Operational Environment and the Changing Character of Future Warfare" (U.S. Army Training and Doctrine Command, May 31, 2017), 11.

[748] Chekinov and Bogdanov, "The Nature and Content of a New-Generation War."

[749] People's Liberation Army, "顺应军事变革潮流把握改革主动 - 中国军网-军报记者," January 5, 2016, http://jz.chinamil.com.cn/n2014/tp/content_6843416.htm.

[750] Kim Hartmann and Christoph Steup, "The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment," n.d., 2.

spoofed GPS data combined with jamming of US GPS signals allowed the Iranians to provide overriding coordinates[751]. This form of protocol compromise was effectively an event-based attack against the Sentinel, conducted by a second-tier regional power. The potential for more intricate attacks against autonomous platforms by more capable parties is significant.

With a rich array of sensory and external inputs, unmanned systems are intrinsically vulnerable to external compromise. Sensors can be fooled to produce erroneous analysis, while external data sources such as command and control, guidance, and telemetry can be overtaken to fool a platform into behaving unexpectedly. Consequently, an overreliance on drones could eventually create new centres of gravity in their command and control centres. If military power is increasingly facilitated by remote operation centres guiding fleets of mixed autonomous platforms, targeting these centres becomes a viable method to reduce adversary fighting strength.

The issue of targeting unmanned command and control is further exasperated by the introduction of so-called "swarming" tactics. Rather than relying on a limited number of potent high-cost systems, militaries may opt to instead deploy cheap formations in high quantity, overwhelming defenders. As a thorough RAND publication from explained as early as 2000, swarming is not uniquely related to unmanned systems and has been applied by human forces for centuries with variable success[752]. The tactic allows remediating asymmetries against well-resourced or massed adversaries with comparatively lesser efforts. Such an approach is already a significant component of Iranian doctrine for dealing with the United States and Israel[753]; it is a component of modern Chinese doctrine[754]; it was used by jihadi forces in Syria to overwhelm deployed Russian forces[755]; and is actively pursued by the United States via DARPA[756].

Unmanned swarms require an increased degree of autonomy as agility becomes essential. Individual warfighters would need to respond rapidly to changes in their surroundings, adversaries, and coordinate with adjacent and remote systems. This will be made possible by extensive mesh networks governed by intricate software. Ostensibly, operational oversight would in the near future remain in the hands of human operators, but those would not be able to directly pilot the dozens or hundreds of drones participating in any given swarm. Autonomous piloting authority would be transferred to the system itself, further extending its vulnerabilities.

Event-based attacks against deployed swarms may be devastatingly effective. By disrupting sensory flow, interfering with telemetry and command channels, or even sending contradictory data to the participating drones, it may be possible to achieve a wide range of effects previously infeasible

---

[751] Hartmann and Steup, 7.

[752] Sean J. A. Edwards, *Swarming on the Battlefield: Past, Present, and Future* (Santa Monica, CA: Rand, 2000).

[753] Brett Davis, "Learning Curve: Iranian Asymmetrical Warfare and Millennium Challenge 2002" (Center for International Maritime Security, August 14, 2014), http://cimsec.org/learning-curve-iranian-asymmetrical-warfare-millennium-challenge-2002-2/11640.

[754] Kania, Elsa, "Swarms at War: Chinese Advances in Swarm Intelligence," Jamestown, July 6, 2017, https://jamestown.org/program/swarms-war-chinese-advances-swarm-intelligence/.

[755] Sanchez, "Russia Uses Missiles and Cyber Warfare to Fight off 'swarm of Drones' Attacking Military Bases in Syria."

[756] Kyle Rempfer, "DARPA Hopes to Swarm Drones out of C-130s in 2019 Test," *Air Force Times*, December 19, 2017, https://www.airforcetimes.com/newsletters/daily-news-roundup/2017/12/18/darpa-hopes-to-swarm-drones-out-of-c-130s-in-2019-test/.

against deployed manned forces that rely on both machine-fed data and their own deduction and contextual situational awareness. The potential for presence-based attack is similarly broad; targeted operations against theatre command centres used to govern drones or against the communication infrastructure used to facilitate control of swarms may confer significant advantages to an adversary.

It is possible that as unmanned systems proliferate in quantity and significance to modern societies, the spectrum of network warfare will commensurately shift. Where today even impactful network intrusions are often discarded as unworthy of countermeasures by the victim, the future may alter this calculus. If unmanned systems become a new form of critical infrastructure, even non-offensive intrusions against the networks that house them may spark grave alarm in victims. The dangers of the cybersecurity dilemma as posited by Buchanan[757] may be irreversibly aggravated – it is impossible to determine whether breaches against networks encompassing autonomous systems and artificial intelligence are meant for intelligence collection or a corruptive attack.

Cyber as a Domain

The story of "cyber" as a domain of war stretches back less than a century. Even as its roots trace back to Norbert Wiener's notion of cybernetics as the persistent relationship between humanity and machines[758] it already becomes tenuous to envision networks as a separate manmade cyberspace, detached from other aspects of humanity and subject to its own rules. The inverse is the reality; the more networks became integrated into other aspects of warfare, the more they became intricately bound to war's innately human circumstances.

It is unlikely that information and the medium that bears it will fade into obscure irrelevance. A retreat into connectionless warfighting devoid of the ever-present hunger for data seems a remote possibility. Yet, that does not imply that "cyber" will necessarily remain as a distinct domain or warfare, or even as a pervasive term. As networks fully permeate warfare, they may simply become implied. Military planners already struggle when accounting for the interplay of networks and the other domains; information seems to seep into the all aspects of warfare, muddling the forced attempts at separation. As this exasperates, attempting to distil a perception of warfare in the so-called fifth domain will become more difficult. MONOs of varying types and intensities may eventually find their way into an integrative doctrine, but they do not inherently require the benefits that domainhood provides, and may indeed suffer from it. Irrespective of the assumed increased susceptibility to network attacks, the ability of network operations to coerce would arguably remain limited. In such a scenario, MONOs will maintain their dependence on the physical domains for pursuing objectives, as a network attack against a defender would predominantly be followed by a kinetic force meant to subdue it.

---

[757] Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*.
[758] Rid, *Rise of the Machines: The Lost History of Cybernetics*, 47–49.

The idea that cyber will not retain its domainhood is not revolutionary. Many other nations – primarily non-Western – already do not envision computers, the networks they form, or the logical entities they create as a separate domain of war. While nations prolific in network operations such as Russia, China, Iran and Israel have an aggressively proactive view of MONOs as a key enabler of modern military success, they primarily view the operational space as information-led, and tasked with enabling broader strategic goals or kinetic operational forces. In this sense, the strategic perspective comparison between east and west differs from the Cold War. As the US focused on a potent air force and absolute technological supremacy, the Soviet Union focused on tight air defence grids, potent rocketry, and proliferation of affordable equipment to global allies. Today, global contenders large agree that information is pivotal to succeed in modern warfare, and that qualitative technological superiority is essential. It is how this technology interplays with the existing tenets of warfare that differs. Where the US and its NATO allies invest in the uniqueness of cyberspace, others espouse holistic warfare through which information is a constant, unrelenting, and crucial undercurrent.

Regardless, MONOs as presented within this thesis are independent of the status of cyber as a domain. Whether carried out by a dedicated military command, intelligence agency, a theatre command centre, or an individual aircraft, the characteristics remain much the same. The operational cycles that enable MONOs require a grand commitment of staff, resources, intelligence, and research. These do not necessarily need to be delivered by a dedicated domain structure, as indeed is the case for many militaries globally. As such, the models presented within this thesis on the integration of MONOs to military doctrine and strategy perform equally whether observing cyberspace as a domain or grasping information holistically. As long as their requirements and parameters are considered and weaved into the decision-making process, they may prove their utility today or in the foreseeable future. The approach to networks may differ as maturity increases, but their characteristics remain largely similar.

CONCLUSIONS

MODELS AS SCAFFOLDING

Cyber-security is naturally a multi-disciplinary field. At its core, the field often reflects the intersection of securing networks with all other domains of study and practice. Cyber is where networks meet criminality, health, safety, finance, commerce, sociology and psychology. As a corollary, cyber-warfare is the intersection of military thought and network security. In cyber, technical and operational aspects are uniquely inseparable and equal in importance; we cannot and should not separate them, or favour one over the other in analysis. Sophisticated offensive and defensive capabilities developed without being understood by their designated users will remain unused, or perhaps misused. Similarly, military strategy that does not account for the radical changes in the operational environment over the last two decades would find itself lacking, even against seemingly disadvantaged adversaries. A reliance on warfare spearheaded by cutting-edge technology must reconcile the vulnerabilities that it creates. These will increasingly be preyed upon by others.

It is easy to label network incidents incorrectly. Some media coverage of high-profile incidents involving networks remains laden with hyperbole, despite a positive trend towards nuance. Security researchers worldwide routinely lament the lacklustre progress in adopting even basic protections, and companies continue to get breached over basic lapses in security. Password reuse, unpatched systems, misconfigured networks, and susceptibility to phishing remain potent ways of compromising even seemingly secure environments. When so many malicious activities occur within the research space, it may become difficult to identify the subtler interplay of network operations and military activities.

Not all network intrusions are attacks, and not all attacks are warfare. While humanity has millennia of experience in distinguishing between malicious activities in the physical domains, the struggle yet continues for distinctions in activity targeting networks. Recognising the differences is significant not only for policy or law-centric analysis, but also for the military domain. Determining which activities could reasonably be assigned to military agencies and units and which should remain civilian is key. Determining which activities are included when discussing national approaches to military approaches is crucial.

Even the perception of cyber itself varies wildly. Some – such as the US and its allies – codify cyber as a domain of warfighting and establish distinct commands to tackle it. Russia adopts a more pragmatic approach to MONOs, viewing them as a fragment of activity within a far broader scope of information operations occurring in both peacetime and conflict. It is a way of achieving or approaching objectives with reduced friction and chances of kinetic escalation. For China, network operations of varying kinds are key facilitators of their modern doctrine, which envisions rapidly

reducing Western technological advantages in any conceivable way. There is no distinctly right or wrong approach, rightness is a measure determined by context. Part of the advantage of network operations lies in their flexibility; they may be applied in many ways against an adversary depending on the circumstance.

The core argument was presented that viewing offensive network capabilities as a monolithic stretch of operational space is risky and counterproductive. Though they differ, Russian, US, and Chinese doctrine primarily treat MONOs as a single spectrum of possibilities that share most characteristics. Yet, network operations were not all created equal. Some may be instantly deployed on the battlefield by an infantry detachment, while others would be carefully managed, multi-year operations against sensitive adversary command centres. On the other, most offered taxonomies splice network operations across numerous variables and parameters, making them useful for post-hoc academic analysis but more limited in utility for military planners. The goal of this thesis was therefore not to generate models that cover every manifestation of operating against networks – though that certainly has its value.

Cyber did not wink into existence overnight. Operations carried out today are a natural result of counter-innovation cycles that have accelerated in the twentieth century. The need to deceive and manipulate the machines on which we have become reliant intensified when militaries turned to radar for guidance and the radio for communication. As these technologies proliferated and became complex, the desire to target them and the possibility to gain value from doing so commensurately increased. This intangible warfare became doubly important as computer networks became an intangible crutch within modern warfighting, one deeply reliant on ever-active datalinks providing sensory data, command and control, and telemetry. Any models pertaining to network warfare must therefore account for their roots in electronic warfare and signals intelligence; cyber is essentially their technological lovechild.

The goal was therefore to craft models which categorise cyber operations in useful ways. By dividing MONOs into event-based and presence-based operations, immediate fault lines begin to surface. When subjecting each of these high-level categories to the operational process underpinning all MONOs, it becomes clear just how much they differ, and how risky it is therefore to bundle them together. Event-based operations are primarily robust, multi-use capabilities requiring high reliability and intensive research and development cycles. Conversely, presence-based operations require permanent intelligence support, covert operational nuance, and would likely eventually compromise themselves upon use. The former befits use with deployed forces, while the latter may be best retained by intelligence agencies with an operational mandate.

This thesis sought to create a robust perspective on MONOs in accumulative layers. Each layer was meant to focus discussion, exclude possibilities that muddle analysis, and offer straightforward classification criteria that are easy to implement both in subsequent research but also in strategy for employing offensive network operations. Each of the four chapters offers self-sufficient analysis from a different perspective. When combined, they indicate that cyber operations can tremendously benefit

from implementing lessons from other forms of technology-focused warfare. A clear typology for offensive network capabilities can then assist in further development of the overall field, by facilitating examination of how each category can be incorporated into strategy, operations, and tactics.

Chapter one examined the spectrum of network operations, setting boundaries around the conceptual perimeter of cyber-warfare. The chapter was intended to narrowly focus the debate itself in a two-pronged approach. The first exercise included identifying which incidents do not merit examination within the prism of offensive network operations undertaken by parties involved in warfare. This excluded a broad range of activities frequently encountered within the debate, such as intelligence collection, criminal activities, information operations, or loosely affiliated ideological hacking. The second exercise sought to offer five escalating criteria which in turn help assess which malicious incidents are worthy of inclusion within the observed dataset. This has the significant side benefit of illustrating how the vast majority of malicious incidents assessed today should likely not be labelled as cyber-warfare.

Chapter two surveyed how each of the main characteristics of MONOs are thoroughly rooted in historic intangible warfare. The twentieth century demonstrated how a rapidly growing reliance on the electromagnetic spectrum initiated a process that culminated in what is now labelled cyber operations. From jamming, to electronic warfare, to command and control and network-centric warfare, each of these iterations of intangible warfare contributes characteristics that accompany modern cyber capabilities. By presenting how MONOs draw from an existing strong foundation, further research can be made on integrating electronic warfare and MONOs along their parallels.

Chapter three introduced the distinction between MONO archetypes – event-based and presence-based operations. The argument was that these two categories are both simple enough to be easily usable while disparate enough to be useful. Event and presence-based capabilities were shown to have distinct characteristics across the entire operational lifecycle. The resource requirements are often unique, the development process differs, targeting is undertaken with different goals in mind, and even the operational staff itself may be altogether distinct. As such, lumping these two operation types together may result in overly broad results.

Chapter four dissected the utility of event and presence-based operations. The goal was to interleave the characteristics of the two MONO archetypes with strategic considerations to determine when, where, how and why they should be used. By examining how pre-existing strategic wisdom remains wholly applicable to cyber-operations, it became clear that event-based capabilities would usually fit tactical or operational needs, while presence-based operations are often best suited for strategic support and pursuit of loftier objectives.

While each of the major powers relies on network operations to a degree, they do so imperfectly. Assessing the various ways key nations fall short of optimally utilising MONOs was the goal of the subsequent three chapters. The United States exhibits top-tier technical capabilities but a limited capacity to operationalise them across all operational spaces due to bureaucratic difficulties, extreme compartmentalisation, and a siloing of MONOs within a separate military command. Capabilities

therefore exist, but are often not applied where they are needed most. Russia is the most visibly aggressive user of MONOs globally, but does so with reckless abandon and little consideration to their overall impact on the underlying military-political objectives. Success is often incidental, limited, or a result of committing to operations in low-quality bulk. Russia has integrated MONOs so thoroughly that they are treated as simply another tool in the information-operations toolset, with narrow regard to how they could be more nuanced in order to pursue more intricate goals. China appears relatively doctrinally mature with a cohesive structure amalgamating cyber-capabilities from across different branches, but a desire to view the information space holistically is not yet backed up with any profound operational experience. Each nation could benefit thoroughly from embedding the characteristics of MONOs into their doctrine, and thoughtfully construct strategy that befits their unique situation.

While a generic model was offered, implementation may still vary. Much like other aspects of military strategy, there is no one optimal approach. Smaller militaries such as the Israeli Defense Forces may focus heavily on event-based capabilities meant to support its strategically crucial air force, while at the same time engaging in presence-based operations to soften adversaries and impact their readiness. Taiwan may disproportionately focus on presence-based operations against the PLA Rocket Force or regional command and control, in efforts to sufficiently delay any PLA advancement so that US forces or the international community may interdict in any attempt to subdue it. Iran may increase its reliance on strategic event-based operations against critical targets within asymmetrically stronger adversaries in order to weaken political resolve and act as a de-facto deterrent. MONOs can act as either a force multiplier, an operational enabler, or even as limited means of pursuing objectives; it all rests on context.

The degree to which nations may rely on MONOs may also understandably vary. An attempt to overly emphasize MONOs in Israeli campaigns against the Palestinian Hamas may be fruitless. While they do rely on information infrastructure, Hamas doctrine broadly assumes distrust in its own equipment and even a total command disconnect when conflict ensues[759]. While the PLA may enjoy some success in subduing a Taiwanese attempt at organising defensive efforts by degrading their command and control, the island campaign would still incorporate multiple layers of entrenched defenders fighting bitterly and autonomously regardless of available networks[760].

MONOs are not one size fits all. The models developed in this thesis are meant to be partially abstract and broadly scoped. This allows flexibility in implementation, one that draws from the particularities that characterise situational parameters. It also means that extrapolation is risky and must be undertaken with care. What has been seen is not necessarily indicative of what will come next. The prime example for this is Stuxnet; there has been no further public disclosure of similar incidents incorporating deceptive presence-based operations against energy facilities to deter nuclear

[759] Elad Popopvich, "A Classical Analysis of the 2014 Israel-Hamas Conflict," *CTC Sentinel* 7, no. 11 (November 2014): 20–24.
[760] Easton, *The Chinese Invasion Threat*, 132.

aspirations of rogue nations[761]. What followed Stuxnet was an array of high-profile destructive attacks against critical infrastructure such as in Ukraine, often used as a tool for political signalling rather than a true ploy to covertly influence adversary grand strategy. Any further analysis of cyber operations must therefore be tightly paired to the specific scenario being assessed.

Future Research

This thesis focused on introducing and testing core concepts for military use of network operations. As such, it leaves many areas relatively undeveloped yet primed for future work. As the use of MONOs evolves and more public evidence provided, the role of these capabilities must be consistently re-evaluated. Each of the conceptual aspects introduced in the thesis may be further developed with additional works, including those that explore the implementation of event and presence-based capabilities, MONOs in low-intensity conflict, the use of MONOs by sub-national fighting groups, and the use of network operations by other actors not considered within this work. It is also advisable to pursue research into the next "swing" of the innovation cycle, which would bring forth autonomous platforms and artificial intelligence into the set of considerations.

The United States has been embroiled in decades of low-intensity combat operations against disparate enemies. Priorities have begun to shift back towards preparing for conflict with near-peer adversaries only over the last few years in light of a resurgent China and an increasingly belligerent Russia. Israel, Russia, the United States, Saudi Arabia, and others have been combating irregular or sub-national groups in the Middle-East and elsewhere. While briefly touched on within this thesis, the specific considerations for using both event and presence-based MONOs against irregular forces could be explored in depth. These groups are often reliant on civilian infrastructure and a mismatching set of appropriated tactical equipment. As such, they are both more and less vulnerable to different types of operations. An analysis of effective MONO use against sub-national groups could contribute greatly towards the robust understanding of offensive network capabilities as a whole.

Flipping that, it is also imperative to assess how sub-national groups may employ network operations. These are already occurring in limited forms, with Hamas and Hezbollah known to undertake limited offensive network operations against Israel in times of conflict[762]. While both groups enjoy a measure of autonomy and access to resources, they are inherently disadvantaged when it comes to acquiring manpower and facilitating the high-cost operational cycles that MONOs commonly entail. It thus becomes useful to explore how low-cost, high-yield MONOs may be attained by such groups, what targets they are likely to pursue, and how they may incorporate such capabilities to enable and augment their accomplishments in the kinetic space.

---

[761] One notable but indeterminate exception is the alleged efforts to curtail North Korean ballistic missile tests by way of MONOs against the associated infrastructure, see Sanger and Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles."

[762] See for example Ben Schaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review* (blog), March 11, 2018, http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

Examining the integration of MONOs into the strategy of other nations would also contribute to a broader understanding of the toolset. North Korea is a prolific user of network operations in pursuit of its grand strategy, making it a prime candidate for case study analysis. Iran is similarly prolific in using offensive network capabilities, either to project coercive political power or to degrade its enemies. With a penchant for network operations and an integrative approach to technological warfare, Israel remains a prime case study for any use of MONOs against adversaries. Implementing the assessment models offered in this thesis against the countries may both strengthen their validity and also offer additional insights unobtainable from observing relatively unshackled global powers.

Trends must consistently be accounted for and incorporated into any assessment. While some aspects of network operations have remained static over the last two decades, technological adoption and development have radically changed. With technologies set to enmesh even further into modern life and gradually increase in autonomy, they may adversely impact both the significance of MONOs and how they are carried out. Timespans are notoriously difficult in technology, so it remains challenging to tell when artificial intelligence would become crucial to this field. The trajectory, however, is clear. Humanity has already peaked in its ability to process the reams of data that networks provide and relies heavily on software to assist. With more data, sensors, and requirements, the need to delegate a greater portion of analytical processes to increasingly intelligent software is becoming clearer.

Autonomous platforms may both target and be targeted through networks. The more computerised these platforms become, the more our overall network attack surface increases. Similarly, such platforms may deliver offensive payloads of their own, potentially assisting in acquiring access to air-gapped networks within well-defended territories. The implication of autonomous platforms should therefore be gradually explored as their adoption increases and data emerges; they may increasingly become a significant component in MONOs, both as target and offensive platforms.

The future role of artificial intelligence in MONOs is indeterminate. As with autonomous platforms, they may both be targets or a vehicle for offensive operations. Much like the adoption of networks and computers, a gradual dependency on artificial intelligence may emerge as they become more adept at solving complex tasks and achieving optimal battlefield results. This may extend to all tiers of military thought; the tactical, operational, and strategic. Where tactical, limited-scope AI may assist in situational-responsive weapons guidance, strategic AI may help direct resources and operational planning at the theatre level. At the same time, other forms of narrow AI may also be used to scale the use of MONOs, effectively shrinking the resource constraints detailed in the operational life-cycle. In adherence to the cyclical mentality, narrow AI may also be used for network defence, thereby drastically reducing the success rate of deterministic approaches to MONOs so often relied upon. All such applications – and their potentially unique impact – could be thoroughly explored in further research.

Finally, defensive operations are crucial to operating in and against networks. While they were largely excluded from this thesis, assessing the offense-defence balance would make for a valuable

supplement. The various strategic approaches to MONOs can and should be countered with risk mitigation approaches. These include a frank reconsideration of the Western approach to technology-laden superiority, in which equipment is often superfluously networked. As a response to the utility of MONOs presented in this thesis, perhaps it would be wise to consider the vulnerability of certain platforms and systems prior to networking them. This type of analysis is particularly relevant in light of some ongoing debates, such as the ongoing debate in regards to the US nuclear arsenal[763].

This thesis generates some answers with those potentially leading to numerous additional questions. If strategic planners and military analysts more thoroughly understand the utility of MONOs, they may do better to gear the analytical conversation and doctrinal construction towards the right questions. One certainty is that networks will both retain and increase their prevalence in all military affairs. Recognising this, it is essential to continuously challenge how MONOs are used and offer additional questions meant to advance their study to as of yet uncharted areas.

[763] Debates are ongoing as to how networked should it be after a much-needed refurbish. For a comprehensive report on the overall attack surface for the arsenal, see Bezya Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities, and Consequences" (Chatham House, January 2018).

CITED WORKS

Books, Book Chapters, and Monographs

Ablon, Lillian. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Santa Monica: RAND Corporation, 2017.

Adamsky, Dmitry. *Cross-Domain Coercion: The Current Russian Art of Strategy*. Institut français des relations internationales, 2015. http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series. Washington, DC: National Defense University Press, 1999.

Arquilla, John. "Ethics and Information Warfare." In *Strategic Appraisal: The Changing Role of Information in Warfare*, edited by Zalmay Khalilzad, John P. White, and Andrew Marshall, 379–401. Santa Monica, CA: RAND, 1999.

Bērziņš, Jānis. "Russian New Generation Warfare Is Not Hybrid Warfare." In *The War in Ukraine: Lessons for Europe*, edited by Artis Pabriks and Andis Kudors, 40–51. Rīga: The Centre for East European Policy Studies : University of Latvia Press, 2015.

Buchanan, Ben. *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press, 2017.

Burton, Robert W., Frank L. Cloutier, Clarence S. Summers, Elliott R. Brown, and John A. Zingg. *The Strategy of Electronic Warfare*. U.S. Air Force Academy, 1979.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco, 2010.

Clausewitz, Carl Von. *On War*. 3rd ed. Vol. 1. London: N. Trubner & Co, 1873.

Conti, Gregory, and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*, 2017.

Cordesman, Anthony H, Ashley Hess, Nicholas S Yarosh, and D.C.) Center for Strategic and International Studies (Washington. *Chinese Military Modernization and Force Development: A Western Perspective*. Washington, D.C.: Center for Strategic and International Studies, 2013.

Crowdy, Terry. *The Enemy Within: A History of Spies, Spymasters and Espionage*. Bloomsbury Publishing, 2011.

Denning, Dorothy E. *Information Warfare and Security*. 4th ed. Reading: Addison-Wesley, 1999.

Douhet, Giulio. *The Command of the Air*. USAF Warrior Studies. Washington, D.C: Office of Air Force History, 1983.

Easton, Ian. *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia*. 1st ed. Arlington, Virgina: Project 2049 Institute, 2017.

Edwards, Sean J. A. *Swarming on the Battlefield: Past, Present, and Future*. Santa Monica, CA: Rand, 2000.

Freedman, Lawrence. *Strategy: A History*. 1. iss. as an Oxford Univ. Press paperback. Oxford: Oxford Univ. Press, 2015.

Fuller, J.F.C. *The Foundations of the Science of War*. Hutchinson & Company, 1926.

Giles, Keir, NATO Defense College, and Research Division. *Handbook of Russian Information Warfare*. Rome, Italy: NATO Defence College Research Division, 2016.

Goertzel, Ben, and Cassio Pennachin, eds. *Artificial General Intelligence*. Cognitive Technologies. Berlin ; New York: Springer, 2007.

Grau, Dr Lester W, and Charles K Bartles. *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces*. Fort Leavenworth: Foreign Military Studies Office, 2016.

Greathouse, Craig B. "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" In *Cyberspace and International Relations*, edited by Jan-Frederik Kremer and Benedikt Müller, 21–40. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

Green, Michael, Ernest Bower, and Center for Strategic and International Studies. *Asia-Pacific Rebalance 2025: Capabilities, Presence, and Partnerships : An Independent Review of U.S. Defense Strategy in the Asia-Pacific*, 2016.

Howard, Michael. “How Much Can Technology Change Warfare?” In *Two Historians in Technology and War*. Carlisle Barracks, PA: US Army War College, 1994.
Hura, Myron, Gary McLeod, James Schneider, Daniel Gonzales, Daniel M. Norton, Jody Jacobs, Kevin M. O’Connel, William Little, Richard Mesic, and Lewis Jamison. “Tactical Data Links.” In *Interoperability: A Continuing Challenge*, 107–21. Chapter 9 - Tactical Data Links: RAND, 2000.
Kramer, Franklin D, Lauren Speranza M, Atlantic Council of the United States, and Brent Scowcroft Center on International Security. *Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework*, 2017. http://www.atlanticcouncil.org/images/publications/Meeting_the_Russian_Hybrid_Challenge_web_0530.pdf.
Kuehl, Dan, and Leigh Armistead. “Information Operations: The Policy and Organizational Evaluation.” In *Information Operations*. Washington D.C.: Potomac Books, 2007.
Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. PLA Literature and Arts Publishing House Arts, 1999.
Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.
———. *What Is Information Warfare?* 3rd edition. Washington DC: National Defense University, 1995.
Liddell Hart, B.H. *Strategy*. 2nd rev. ed. New York, N.Y., U.S.A: Meridian, 1991.
Lostumbo, Michael, David R. Frelinger, James Williams, and Barry Wilson. *Air Defense Options for Taiwan: An Assessment of Relative Costs and Operational Benefits*. Research Report, RR-1051-OSD. Santa Monica, California: Rand Corporation, 2016.
Mahan, Alfred Thayer. *The Influence of Sea Power upon History, 1660-1783*. Read Books Ltd, 2013.
McDevitt, Michael. “The PLA Navy’s Antiaccess Role in a Taiwan Contingency.” In *The Chinese Navy*, edited by Phillip C. Saunders, Christopher Yung, Michael Swaine, and Andrew Nien-Dzu Yang. Washington DC: Institute for National Strategic Studies, 2011.
Midson, David. “Geography, Territory and Sovereignty in Cyber Warfare.” In *New Technologies and the Law of Armed Conflict*, edited by Hitoshi Nasu and Robert McLaughlin, 75–93. The Hague: T.M.C. Asser Press, 2014.
Monte, Matthew. *Network Attacks & Exploitation: A Framework*. Indianapolis, IN, USA: John Wiley & Sons, Inc, 2015.
Price, Alfred. *Instruments of Darkness*. Barnsley, UK: Frontline Books, 2017.
Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, Mass: MIT Press, 2001.
Rattray, Gregory J., and Jason Healey. “Categorizing and Understanding Offensive Cyber Capabilities and Their Use.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington D.C.: National Academic Press, 2010.
Rid, Thomas. *Rise of the Machines: The Lost History of Cybernetics*. Scribe Publications, 2016.
Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.
Tikk, Eneken, Kadri Kaska, Liis Vihul, and NATO Cooperative Cyber Defence Centre of Excellence. *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010.
Tzu, Sun. *The Art of War*. 2004th ed. Sheba Blake, n.d.
Waltz, Kenneth. *Man, the State, and War: A Theoretical Analysis*. Columbia University Press, 2013.
Williams, Kieran. *The Prague Spring and Its Aftermath: Czechoslovak Politics, 1968-1970*. 1st ed. Cambridge, United Kingdom: Cambridge University Press, 1997.
Wortzel, Larry M. “PLA ‘Joint’ Operational Contingencies in South Asia, Central Asia, and Korea.” In *Beyond The Strait: PLA Missions Other Than Taiwan*, edited by Roy Kamphausen, David Lai, and Andrew Scobell. Carlisle, PA: Strategic Studies Institute, 2009.
寿晓松, 军事科学院, and 军事战略研究部. *The Science of Military Strategy*. 北京: 军事科学出版社, 2013.

Journal Articles and Conference Proceedings

Arquilla, John, and David Ronfeldt. “Cyberwar Is Coming!” *Comparative Strategy* 12, no. 2 (1993): 141–65.
Ayoub, Kareem, and Kenneth Payne. “Strategy in the Age of Artificial Intelligence.” *Journal of Strategic Studies* 39, no. 5–6 (September 18, 2016): 793–819.

Barrett, Neil. “Penetration Testing and Social Engineering: Hacking the Weakest Link.” *Information Security Technical Report* 8, no. 4 (2003): 56–64.
Bartles, Charles K. “Getting Gerasimov Right.” *Military Review* 96, no. 1 (2016): 30–38.
Baylev, Col S I, and Col I N Dylevsky. “The Russian Armed Forces in the Information Environment: Principles, Rules, and Confidence-Building Measures,” n.d., 6.
Bennett, David. “An Analysis of the China’s Offshore Active Defense and the People’s Liberation Army Navy.” *Global Security Studies* 1, no. 1 (2010). http://globalsecuritystudies.com/Bennett%20China.pdf.
Bronk, Christopher, and Eneken Tikk-Ringas. “The Cyber Attack on Saudi Aramco.” *Survival* 55, no. 2 (May 2013): 81–96.
Brooks, Teresa Nicole. “Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems.” *ArXiv:1702.06162 [Cs]*, February 20, 2017. http://arxiv.org/abs/1702.06162.
Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, et al. “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.” *ArXiv:1802.07228*, February 2018.
Burbank, Jack L., Philip F. Chimento, Brian K. Haberman, and William T. Kasch. “Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology.” *IEEE Communications Magazine* 44, no. 11 (2006).
Campbell, Murray, A Joseph Hoane Jr, and Feng-hsiung Hsu. “Deep Blue.” *Artificial Intelligence* 134, no. 1–2 (2002): 57–83.
Cebrowski, Arthur K., and John J. Garstka. “Network-Centric Warfare: Its Origin and Future.” In *US Naval Institute Proceedings*, 124:28–35, 1998.
Chekinov, Sergey G., and Sergey A. Bogdanov. “The Nature and Content of a New-Generation War.” *Military Thought* 4 (2013): 12–23.
Clarke, Richard A. “War From Cyberspace.” *The National Interest*, 2009, 31–36.
Cliff, Roger. “Anti-Access Measures in Chinese Defense Strategy.” *Testimony before the US-China Economic and Security Review Commission*, 2011. http://162.140.209.1/sites/default/files/1.27.11Cliff.pdf.
Cockburn, Robert. “The Radio War.” *IEE Proceedings A-Physical Science, Measurement and Instrumentation, Management and Education-Reviews* 132, no. 6 (1985): 423–434. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4647746.
Cohen, Eliot A. “A Revolution in Warfare.” *Foreign Affairs* 75, no. 2 (1996): 37–54.
Deeks, Ashley. “The Geography of Cyber Conflict: Through a Glass Darkly,” 2013.
Deibert, R. J., R. Rohozinski, and M. Crete-Nishihata. “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War.” *Security Dialogue* 43, no. 1 (February 1, 2012): 3–24. http://sdi.sagepub.com/cgi/doi/10.1177/0967010611431079.
Dekker, Anthony H. “Measuring the Agility of Networked Military Forces.” *Journal of Battlefield Technology* 9, no. 1 (2006): 19.
Ducheine, Paul, and Jelle van Haaster. “Fighting Power, Targeting and Cyber Operations.” In *6th International Conference On Cyber Conflict*, 303–327. IEEE, 2014. http://ieeexplore.ieee.org/abstract/document/6916410/.
Farwell, James P., and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (February 2011): 23–40.
Felt, Adrienne Porter, Richard Barnes, April King, Chris Palmer, Chris Bentzel, and Parisa Tabriz. “Measuring HTTPS Adoption on the Web.” In *26th USENIX Security Symposium*, 1323–1338, 2017.
Forcese, Craig. “Spies Without Borders: International Law and Intelligence Collection.” *Journal of National Security Law and Policy* 5 (2011).
Fortun, M., and S. S. Schweber. “Scientists and the Legacy of World War II: The Case of Operations Research.” *Social Studies of Science* 23 (1993): 595–642.
Futter. “The Dangers of Using Cyberattacks to Counter Nuclear Threats.” *Arms Control Today* 46, no. 6 (2016): 8–14.
Gerasimov, Valery. “The Value of Science Is in the Foresight.” *Military Review* 96, no. 1 (2016): 23.
Gerges, Fawaz A. “The Obama Approach to the Middle East: The End of America’s Moment?” *International Affairs* 89, no. 2 (2013): 299–323.
Giles, Keir. “‘Information Troops’-A Russian Cyber Command?” In *3rd International Conference on Cyber Conflict*, 45–60, 2011.
Graham, David E. “Cyber Threats and the Law of War.” *J. Nat’l Sec. L. & Pol’y* 4 (2010): 87. http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jnatselp4&section=10.

Hartmann, Kim, and Christoph Steup. “The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment,” n.d., 23.
Hoffman, Frank G. “Hybrid Warfare & Challenges.” *Joint Forces Quarterly*, no. 52 (2009): 34–47.
Horowitz, Michael C. “Artificial Intelligence, International Competition, and the Balance of Power.” *Texas National Security Review* 1, no. 3 (May 2018): 37–57.
Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” *Leading Issues in Information Warfare & Security Research* 1 (2011): 80.
Hwang, Ji-Jen. “China’s Military Reform: The Strategic Support Force, Non-Traditional Warfare, and the Impact on Cross-Strait Security.” *Issues & Studies* 53, no. 03 (September 2017): 1–25.
Inkster, Nigel. “Conflict Foretold: America and China.” *Survival* 55, no. 5 (October 2013): 7–28.
Jones, Reginald V. “Scientific Intelligence.” *Journal of the Royal United Service Institution* 92 (1956): 352–69.
Kania, Elsa, and Costello, John. “The Strategic Support Force and the Future of Chinese Information Operations.” *Cyber Defense Review* 3, no. 1 (Spring 2018): 105–21.
Katzman, Kenneth, and Paul K. Kerr. “Iran Nuclear Agreement.” *Washington, DC: Congressional Research Service*, 2015.
Korns, Stephen W., and Joshua E. Kastenberg. “Georgia’s Cyber Left Hook.” *Parameters* 38, no. 4 (2008): 60.
Kuznetsov, Lt. Gen. V. I., Col. Yu. Ye. Donskov, and Lt. Col. O. G. Nikitin. “Cyberspace in Military Operations Today.” *Military Thought* 23, no. 1 (2014): 20–25.
Langner, Ralph. “Stuxnet - Dissecting a Cyberwarfare Weapon.” *IEEE Security and Privacy* 9, no. 3 (June 2011): 49–51.
Liddell Hart, B.H. “The Objective in War.” *Naval War College Review* 5, no. 4 (December 1952): 1–30.
Lin, Herbert S. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law and Policy* 4 (2010): 63.
Lincoln Bonner III, E. “Cyber Power in 21st-Century Joint Warfare.” *Joint Forces Quarterly* 74, no. 3 (2014): 102–9.
Lynn, William. “Defending a New Domain - The Pentagon’s Cyberstrategy.” *Foreign Affairs* 89, no. 5 (October 2010): 97–108.
Maruyev, A. Yu. “Russia and the U.S.A in Confrontation: Military and Political Aspects.” *Military Thought* 18, no. 3 (July 1, 2009): 1–8.
Mazanec, Brian M. “The Art of (Cyber) War.” *The Journal of International Security Affairs* 16 (Spring 2009): 81–90.
McGhee, James E. “Liberating Cyber Offense.” *Strategic Studies Quarterly*, Winter 2016, 46–63.
McMaster, H. R. “The Human Element: When Gadgetry Becomes Strategy.” *World Affairs* 171, no. 3 (2009): 31–43.
McMaster, H.R. “On War: Lessons to Be Learned.” *Survival* 50, no. 1 (March 2008): 19–30.
McReynolds, Joe. “China’s Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy.” *China Brief* 15, no. 8 (April 17, 2015): 3–7.
Mead, Walter Russell. “The Return of Geopolitics: The Revenge of the Revisionist Powers.” *Foreign Aff.* 93 (2014): 69.
Moore, Daniel. “Targeting Technology: Mapping Military Offensive Network Operations.” In *2018 10th International Conference on Cyber Conflict (CyCon)*, 89–108. IEEE, 2018.
Nye, Joseph S. “America’s Information Edge.” *Foreign Affairs*, March 1996, 20–36. https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge.
Parks, Raymond C., and Duggan, David P. “Principles of Cyber-Warfare.” In *Proceedings from the Second Annual IEEE SMC Information Assurance Workshop*, 122–26. New York: West Point, 2001.
Perov, Col E A, and Col A V Pereverzev. “On the Prospective Digital Communication Network of the RF Armed Forces.” *Military Thought* 17, no. 2 (2008): 89–95.
Peterson, Dale. “Offensive Cyber Weapons: Construction, Development, and Employment.” *Journal of Strategic Studies* 36, no. 1 (February 2013): 120–24.
Popopvich, Elad. “A Classical Analysis of the 2014 Israel-Hamas Conflict.” *CTC Sentinel* 7, no. 11 (November 2014): 20–24.
Rainey, James W. “Ambivalent Warfare: Tactical Doctrine of the AEF in World War I.” *Parameters* 13, no. 3 (1983): 34–46.
Rid, Thomas, and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37.

Rid, Thomas, and Peter McBurney. “Cyber-Weapons.” *The RUSI Journal* 157, no. 1 (February 2012): 6–13.
Safran, Nadav. “Trial by Ordeal: The Yom Kippur War, October 1973.” *International Security* 2, no. 2 (1977): 133–70.
Schmitt, Michael N. “‘Attack’ as a Term of Art in International Law: The Cyber Operations Context.” In *4th International Conference on Cyber Conflict*, 1–11. IEEE, 2012.
Schneider, James, and Lawrence L. Izzo. “Clausewitz’s Elusive Center of Gravity.” *Parameters*, September 1987, 46–57.
Scott, Roger D. “Territorially Intrusive Intelligence Collection and International Law.” *The Air Force Law Review* 46 (1999): 217–24.
Shimshoni, Jonathan. “Technology, Military Advantage, and World War I: A Case for Military Entrepreneurship.” *International Security* 15, no. 3 (1990): 187.
Smeets, Max. “A Matter of Time: On the Transitory Nature of Cyberweapons.” *Journal of Strategic Studies*, February 16, 2017, 1–28.
Smith, Edward A. “Effects Based Operations.” *Applying Network Centric Warfare in Peace*, 2005.
Snegovaya, Maria. “Putin’s Information Warfare in Ukraine.” *Soviet Origins Of Russia’s Hybrid Warfare, Washington*, 2015.
Strachan, Hew. “The Battle of the Somme and British Strategy.” *Journal of Strategic Studies* 21, no. 1 (March 1998): 79–95.
“Syria: Foreign Intervention Still Debated, but Distant.” *Strategic Comments* 18, no. 6 (August 2012): 1–5.
Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. “Intriguing Properties of Neural Networks.” *ArXiv:1312.6199 [Cs]*, December 20, 2013. http://arxiv.org/abs/1312.6199.
Thomas, Timothy. “Russia’s Reflexive Control Theory and the Military.” *The Journal of Slavic Military Studies* 17, no. 2 (June 2004): 237–56.
Thornton, Rod. “The Changing Nature of Modern Warfare: Responding to Russian Information Warfare.” *The RUSI Journal* 160, no. 4 (July 4, 2015): 40–48.
Tirpak, John A. “Making the Best of the Fighter Force.” *Air Force Magazine* 90, no. 3 (2007): 40. http://www.airforcemag.com/MagazineArchive/Documents/2007/March%202007/0307force.pdf.
Vinod Anand. “Chinese Concepts and Capabilities of Information Warfare.” *Strategic Analysis* 30 (2006): 781–97.
Waltz, Kenneth N. “The Origins of War in Neorealist Theory.” *Journal of Interdisciplinary History* 18, no. 4 (1988): 615.
Wang, Vincent Wei-cheng. “The Chinese Military and the" Taiwan Issue": How China Assesses Its Security Environment.” *Tamkang Journal of International Affairs* 10, no. 4 (2007): 89.
Watson-Watt, Robert. “Battle Scars of Military Electronics - The Scharnhorst Break-Through.” *IRE Transactions on Military Electronics* 1, no. 1 (March 1957): 19–25.
Weinberger, Sharon. “Is This the Start of Cyberwarfare?” *Nature* 474, no. 7350 (2011): 142. http://search.proquest.com/openview/8558e1d85b80b4fabe7a8ae1ae79704b/1?pq-origsite=gscholar&cbl=40569.
Whetten, Lawrence, and Michael Johnson. “Military Lessons of the Yom Kippur War.Pdf.” *The World Today* 30, no. 3 (March 1974): 101–10.
Wilson, Clay. “Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.” DTIC Document, 2007. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA466599.
Wortzel, Larry M. “PLA Command, Control and Targeting Architectures: Theory, Doctrine, and Warfighting Applications.” *Right-Sizing the People’s Liberation Army: Exploring the Contours of China’s Military* 197 (2007). http://kms1.isn.ethz.ch/serviceengine/Files/ISN/48444/ichaptersection_singledocument/8c5607a1-4ad7-46d3-8490-22fc612f3002/en/Chapter%205.pdf.
Zimmerman, Hubert. “OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection.” *IEEE Transactions on Communications* 28, no. 4 (April 1980): 425–32.

Patents

Hershey, Paul C., Joseph O. Chapa, and Elizabeth Umberger. Methods and apparatuses for eliminating a missile threat. United States US20160070674A1, filed September 9, 2014, and issued March 10, 2016.

Hershey, Paul C., Robert E. Dehnert JR, and John J. Williams. Digital weapons factory and digital operations center for producing, deploying, assessing, and managing digital defects. United States US9544326B2, filed January 20, 2015, and issued January 10, 2017.
Hershey, Paul Christian, Marilyn Winklareth Zett, Angelo Cianciosi II Michael, Brianne Rene-Martinek Hoppes, Roland Dige Chang, Andrew Arnold, and John Zolper JR. System and method for integrated and synchronized planning and response to defeat disparate threats over the threat kill chain with combined cyber, electronic warfare and kinetic effects. United States US20180038669A1, filed February 28, 2017, and issued February 8, 2018.
Jahne, Seth L., Blake Jeffrey Harnden, Eric R. Van Alst, James M. Chan, James M. Kalasky, and Andrew Paul Riha. Techniques Deployment System. United States US20150369569A1, filed June 24, 2014, and issued December 24, 2015.
Keegan, Matthew, and Stephen Leonard Engelson Wyatt. Method and system for a small unmanned aerial system for delivering electronic warfare and cyber effects. United States US20180009525A1, filed March 15, 2016, and issued January 11, 2018.
Leibunguth, Jonathon P. Command and Control Systems for Cyber Warfare. United States US20090249483A1, filed March 30, 2009, and issued October 1, 2009.

Reports

Alberts, David S. “Agility, Focus, and Convergence: The Future of Command and Control.” Office of the Assistant Secretary of Defense for Networks and Information Integration, 2007.
Belk, Robert, and Matthew Noyes. “On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy.” Cambridge, Mass: John F Kennedy School of Government, 2012. http://www.dtic.mil/docs/citations/ADA561817.
Bolia, Robert S. “Overreliance on Technology in Warfare: The Yom Kippur War as a Case Study.” DTIC Document, 2004. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA485884.
Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. “The Diamond Model of Intrusion Analysis.” DTIC Document, 2013. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA586960.
Carter, Ash. “A Lasting Defeat: The Campaign to Destroy ISIS.” Cambridge, Mass: The Belfer Center, October 2017.
Caton, Jeffrey, L. “Army Support of Military Cyberspace Operations.” Strategic Studies Institute, January 2015.
Chairman of the Joint Chiefs of Staff. “National Military Strategy for Cyberspace Operations.” Chairman of the Joint Chiefs of Staff, December 2006.
Chotikul, Diane. “The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study:” Fort Belvoir, VA: Defense Technical Information Center, July 1, 1986. http://www.dtic.mil/docs/citations/ADA170613.
Clapper Jr, James R. “Challenging Joint Military Intelligence.” DTIC Document, 1994. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA528900.
Comae. “The Shadow Brokers: Cyber Fear Game-Changers.” Comae Technologies, July 2017.
Connell, Michael, and Sarah Vogler. “Russia’s Approach to Cyber Warfare.” Arlington, VA: CNA, March 24, 2017.
Cordesman, Anthony H. “Chinese Strategy and Military Power in 2014.” Center for Strategic & International Studies, November 2014.
Cummings, M L. “Artificial Intelligence and the Future of Warfare.” Chatham House, January 2017.
Cybereason. “Paying the Price of Destructive Cyber Attacks,” 2017. https://hi.cybereason.com/hubfs/Content%20PDFs/Paying-the-Price-of-Destructive-Cyber-Attacks.pdf?t=1505592823490.
Davis, Brett. “Learning Curve: Iranian Asymmetrical Warfare and Millennium Challenge 2002.” Center for International Maritime Security, August 14, 2014. http://cimsec.org/learning-curve-iranian-asymmetrical-warfare-millennium-challenge-2002-2/11640.
Defense Science Board. “Task Force on Cyber Deterrence.” Department of Defense, February 2017.
Dragos. “CRASHOVERRIDE: Threat to the Electric Grid Operations.” Dragos, June 12, 2017.
Easton, Ian. “Able Archers: Taiwan Defense Strategy in an Age of Precision Strike.” Project 2049 Institute, n.d.
Estonian Foreign Intelligence Service. “International Security and Estonia,” 2018.
Falliere, Nicolas, Liam O Murchu, and Eric Chien. “W32.Stuxnet Dossier.” Symantec, February 2011.
Franke, Ulrik. “War by Non-Military Means,” 2015. http://www.foi.se/ReportFiles/foir_4065.pdf.

Giles, Keir. “Russia’s ‘New’ Tools for Confronting the West.” London, U.K.: Chatham House, March 2016.
GReAT. “The Duqu 2.0: Technical Details.” Kaspersky Lab, June 11, 2015. https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/.
———. “The ProjectSauron APT.” Kaspersky Lab, August 9, 2016. https://securelist.com/faq-the-projectsauron-apt/75533/.
Heickero, Roland. “Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.” Swedish Defence Research Agency, March 2010.
HP Security Research. “Profiling an Enigma: The Mystery of North Korea’s Cyber Threat Landscape.” Hewlett Packard, August 16, 2014.
Hutcherson, Norman B. “Command & Contorl Warfare: Putting Another Tool in the War-Fighter’s Data Base.” Alabama, United States: Air University Press, 1994.
Jane’s. “Exploiting The Network For Smarter Weapon Effects.” Jane’s International Defence Review, August 2015.
Jun, Jenny, Scott LaFoy, and Ethan Sohn. “North Korea’s Cyber Operations.” Center for Strategic & International Studies, December 2015.
Kania, Elsa. “Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power.” Center for a New American Security, November 2017.
Kaspersky Lab. “The Regin Platform: Nation State Ownage of GSM Networks,” November 24, 2014.
Kemp, Herbert C. “Left of Launch: Countering Theater Ballistic Missiles.” Issue Brief. Atlantic Council, July 2017.
King, David R., and Joseph D. Massey. “History of the F-15 Program: A Silver Anniversary First Flight Remembrance.” AIR FORCE LOGISTICS MANAGEMENT AGENCY GUNTER AFB AL, 1997. http://www.dtic.mil/docs/citations/ADA328680.
Lee, Robert M., Michael J. Assante, and Tim Conway. “German Steel Mill Cyber Attack.” SANS ICS, 2014.
Lewis, James A. “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.” Washington, DC: Center for Strategic & International Studies, December 2002.
———. “Thresholds for Cyberwar.” Center for Strategic and International Studies, 2010.
Libicki, Martin C. “Why Cyber Will Not and Should Not HAve Its Grand Strategist.” AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST, 2014. http://www.dtic.mil/docs/citations/ADA602106.
Mandiant. “APT1 - Exposing One of China’s Cyber Espionage Units,” 2013.
Nye, Joseph S. “Cyber Power.” DTIC Document, 2010. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626.
O’Conner, Sean. “Access Denial - Syria’s Air Defence Network.” Jane’s International Defence Review, 2014.
Plucker, Ron C. “Command and Control Warfare - A New Concept for the Joint Operational Commander.” DTIC Document, 1993. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA266700.
SANS Industrial Control Systems, and E-ISAC. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” Washington, DC, March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
Symantec. “Dragonfly: Cyberespionage Attacks Against Energy Suppliers.” Symantec, July 7, 2014.
———. “Internet Security Threat Report.” Symantec, April 2017. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.
Turkish Government. “National Cyber Security Strategy and 2013-2014 Action Plan.” Turkey: Ministry of Transport, Maritime Affairs and Communications, 2013.
Unal, Bezya, and Patricia Lewis. “Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities, and Consequences.” Chatham House, January 2018.
U.S. Department of Defense. “Aegis Modernization Report Program - Fiscal Year 2016.” U.S. Department of Defense, 2017.
———. “Fiscal Year 2015 DoD Programs - F-35 Joint Strike Fighter (JSF).” U.S. Department of Defense, January 2016.
———. “Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF).” U.S. Department of Defense, January 2017.
———. “US National Security Strategy,” December 2017.
U.S. DIA. “Soviet Electronic Countermeasures During Invasion of Czechoslovakia.” U.S. Defense Intelligence Agency, October 1, 1968.
U.S. DNI. “A Common Cyber Threat Framework: A Foundation for Communication.” Office of the Direction of National Intelligence, 2013.

https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf.
U.S. DoD. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China." U.S. Department of Defense, May 15, 2017.
U.S. Navy. "Electronics Technician Volume 03-Communications Systems," July 1997. http://electronicstechnician.tpub.com/14088/css/14088_144.htm.
———. "Report on Collisions Involving USS John McCain and USS Fitzgerald." Office of the Chief of Naval Operations, October 23, 2017.
Van Tol, Jan, Mark Gunzinger, Andrew Krepinevich, and Jim Thomas. "AirSea Battle: A Point-of-Departure Operational Concept." DTIC Document, 2010. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522258.
Verizon. "2018 Data Breach Investigations Report." Verizon, 2018. https://www.verizonenterprise.com/verizon-insights-lab/dbir/.
Zakheim, Dov S. "The United States Navy and Israeli Navy: Background, Current Issues, Scenarios, and Prospects." Center for Naval Assessment, 2012. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA559163.

News Articles, Magazine Articles, and Blog Posts

Alperovitch, Dmitri. "Bears in the Midst: Intrusion into the Democratic National Committee »," June 15, 2016. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.
Barnes, Julian E., and Siobhan Gorman. "U.S. Says Iran Hacked Navy Computers." *Wall Street Journal*, September 27, 2013, sec. World. https://www.wsj.com/articles/us-says-iran-hacked-navy-computers-1380314771.
Bing, Chris, and Patrick Howell O'Neill. "Kaspersky's 'Slingshot' Report Burned an ISIS-Focused Intelligence Operation." *Cyberscoop* (blog), March 20, 2018. https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/.
Bisson, David. "Hacker Admits to Stealing Military Data from U.S. Department of Defense." *Tripwire*, June 16, 2017. https://www.tripwire.com/state-of-security/latest-security-news/hacker-admits-to-stealing-military-data-from-u-s-department-of-defense/.
Bremmer, Ian. "These 5 Facts Explain the Threat of Cyber Warfare." *Time*, June 19, 2015. http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/.
Chirgwin, Richard. "IT 'heroes' Saved Maersk from NotPetya with Ten-Day Reinstallation Bliz." *The Register*, January 25, 2018. https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.
Coker, Margaret, and Paul Sonne. "Ukraine: Cyberwar's Hottest Front." *Wall Street Journal*, November 10, 2015, sec. World. http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.
Costello, John. "The Strategic Support Force: China's Information Warfare Service." *China Brief* (blog), February 8, 2016. https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/.
CrowdStrike. "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units." *CrowdStrike Blog* (blog), December 22, 2016. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.
Drew, Christopher. "Lockheed Says Hacker Used Stolen SecurID Data." *The New York Times*, June 3, 2011, sec. Technology. https://www.nytimes.com/2011/06/04/technology/04security.html.
Drogin, Bob. "Russians Seem To Be Hacking Into Pentagon / Sensitive Information Taken -- but Nothing Top Secret." *Los Angeles Times*, October 7, 1999. https://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php.
Dyer, Geoff. "US Launches Online Assault against Isis." *Financial Times*, April 6, 2016. https://www.ft.com/content/4d98edd0-fba5-11e5-b3f6-11d5706b613b.
Elkind, Peter. "Sony Pictures: Inside the Hack of the Century." *Fortune* (blog), July 1, 2015. http://fortune.com/sony-hack-part-1/.
Faughnder, Ryan, Dave Paresh, and Saba Hamedy. "Hack at Sony Pictures Shuts Computer System." *The Los Angeles Times*, November 24, 2014. http://www.latimes.com/entertainment/envelope/cotown/la-fi-sony-hack-20141125-story.html.

Ferguson, Rik. “TV5 Monde, Russia and the CyberCaliphate.” *Trend Micro* (blog), June 10, 2015. http://blog.trendmicro.co.uk/tv5-monde-russia-and-the-cybercaliphate/.
Franceschi-Bicchierai, Lorenzo. “We Spoke to DNC Hacker ‘Guccifer 2.0.’” *Motherboard*, June 21, 2016. https://motherboard.vice.com/en_us/article/aek7ea/dnc-hacker-guccifer-20-interview.
Freedberg Jr., Sydney J. “ALIS Glitch Grounds Marine F-35Bs.” *Breaking Defense* (blog), June 22, 2017. http://breakingdefense.com/2017/06/breaking-alis-glitch-grounds-marine-f-35bs/.
Freedberg Jr., Sydney J. “Wireless Hacking In Flight: Air Force Demos Cyber EC-130.” *Breaking Defense* (blog), September 15, 2015. https://breakingdefense.com/2015/09/wireless-hacking-in-flight-air-force-demos-cyber-ec-130/.
Frenkel, Sheera. “Experts Say Russians May Have Posed As ISIS To Hack French TV Channel.” *BuzzFeed*, June 10, 2015. https://www.buzzfeed.com/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t.
Galeotti, Mark. “The ‘Gerasimov Doctrine’ and Russian Non-Linear War.” *In Moscow’s Shadows* (blog), July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.
Gallagher, Sean. “F-35 Radar System Has Bug That Requires Hard Reboot in Flight.” *Ars Technica*, March 10, 2016. https://arstechnica.com/information-technology/2016/03/f-35-radar-system-has-bug-that-requires-hard-reboot-in-flight/.
Geller, Eric. “Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand.” *POLITICO*, August 16, 2018. https://politi.co/2MSWCnS.
Giannangeli, Marco. “Russians ‘Hacking into’ RAF Crews over Syria.” *The Daily Express*, January 15, 2017. http://www.express.co.uk/news/world/754236/russia-raf-bombers-syria-hacking-missions-military-army.
Goldman, Adam. “New Charges in Huge C.I.A. Breach Known as Vault 7.” *The New York Times*, June 19, 2018, sec. U.S. https://www.nytimes.com/2018/06/18/us/politics/charges-cia-breach-vault-7.html.
Goodin, Dan. “Group Claims to Hack NSA-Tied Hackers, Posts Exploits as Proof.” *Ars Technica*, August 16, 2016. https://arstechnica.com/information-technology/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/.
Gordon, Michael R. “Despite Cold War’s End, Russia Keeps Building a Secret Complex.” *The New York Times*, April 16, 1996, sec. World. https://www.nytimes.com/1996/04/16/world/despite-cold-war-s-end-russia-keeps-building-a-secret-complex.html.
Gorman, Siobahn, August Cole, and Yochi Dreazen. “Computer Spies Breach Fighter-Jet Project.” *The Wall Street Journal*, April 21, 2009. http://www.wsj.com/articles/SB124027491029837401.
GReAT. “Equation: The Death Star of Malware Galaxy.” *Securelist* (blog), February 16, 2015. https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.
———. “‘Red October’ Diplomatic Cyber Attacks Investigation.” *Kaspersky Securelist* (blog), January 14, 2013. https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/.
———. “The Devil’s in the Rich Header.” *Kaspersky Securelist* (blog), March 8, 2018. https://securelist.com/the-devils-in-the-rich-header/84348/.
Greenberg, Andy. “Ukrainians Say Petya Ransomware Hides State-Sponsored Attacks.” *Wired*, June 28, 2017. https://www.wired.com/story/petya-ransomware-ukraine/.
Hamill, Jasper. “Bank-Busting Jihadi Botnet Comes Back To Life. But Who Is Controlling It This Time?” *Forbes*, June 30, 2014. https://www.forbes.com/sites/jasperhamill/2014/06/30/bank-busting-jihadi-botnet-comes-back-to-life-but-who-is-controlling-it-this-time/#3df4bb0f6f07.
Hauer, Neil. “Russia’s Mercenary Debacle in Syria.” *Foreign Affairs*, February 26, 2018. https://www.foreignaffairs.com/articles/syria/2018-02-26/russias-mercenary-debacle-syria.
Hsu, Jeremy. “The Strava Heat Map Shows Even Militaries Can’t Keep Secrets from Social Data.” *Wired*, January 30, 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.
Johnson, Bobbie. “US Asks China to Explain Google Hacking Claims.” *The Guardian*, January 13, 2010, sec. Technology. https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us.
Jones, Sam. “Ministry of Defence Fends Off ‘Thousands’ of Daily Cyber Attacks.” *Financial Times*, June 25, 2015. https://www.ft.com/content/2f6de47e-1a9a-11e5-8201-cbdb03d71480.
Kopan, Tal. “DNC Hack: What You Need to Know.” *CNN*, June 21, 2016. http://www.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/index.html.

Kopp, Carlo. “JTIDS/MIDS - Network Centric Warfare Fundamentals.” *DefenceTODAY*, n.d.
Kozy, Adam. “Two Birds, One STONE PANDA.” *CrowdStrike Blog* (blog), August 30, 2018. https://www.crowdstrike.com/blog/two-birds-one-stone-panda/.
Lewis, Jeffrey. “Is the United States Really Blowing Up North Korea’s Missiles?” *Foreign Policy* (blog), April 19, 2017. https://foreignpolicy.com/2017/04/19/the-united-states-isnt-hacking-north-koreas-missile-launches/.
Makovsky, David. “The Silent Strike.” *The New Yorker*, September 17, 2012. http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.
Mangosing, Frances. “New Photos Show China Is Nearly Done with Its Militarization of South China Sea.” *Inquirer.Net*, February 5, 2018. http://www.inquirer.net/specials/exclusive-china-militarization-south-china-sea.
Markoff, John. “SecurID Company Suffers Security Breach.” *The New York Times*, March 17, 2011, sec. Technology. https://www.nytimes.com/2011/03/18/technology/18secure.html.
Maynor, David, Aleksander Nikolic, Matt Olney, and Yves Younan. “The MeDoc Connection.” *Cisco Talos* (blog), July 5, 2017. http://blog.talosintelligence.com/2017/07/the-medoc-connection.html.
Mercer, Warren, Paul Rascagneres, and Matthew Molyett. “Olympic Destroyer Takes Aim At Winter Olympics.” *Cisco’s Talos Intelligence* (blog), February 12, 2018. http://blog.talosintelligence.com/2018/02/olympic-destroyer.html.
Miou, Song. “First China-U.S. Cyber Security Ministerial Dialogue Yields Positive Outcomes.” *Xinhua News*, December 2, 2015. http://news.xinhuanet.com/english/2015-12/02/c_134874733.htm.
Morozov, Evgeny. “How I Became a Soldier in the Georgia-Russia Cyberwar.” *Slate*, August 14, 2008. http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.
Nakashima, Ellen, and Craig Timberg. “NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did.” *Washington Post*, May 16, 2017, sec. Technology. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.
Paletta, Damian, Danny Yadron, and Jennifer Valentino-DeVries. “Cyberwar Ignites a New Arms Race.” *Wall Street Journal*, October 12, 2015, sec. World. http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128.
Perlroth, Nicole. “Cyberattack Caused Olympic Opening Ceremony Disruption.” *The New York Times*, February 13, 2018, sec. Technology. https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html.
Perlroth, Nicole, and Quentin Hardy. “Online Banking Attacks Were Work of Iran, U.S. Officials Say.” *The New York Times*, January 8, 2013. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
Perlroth, Nicole, and Savage, Charlie. “Is D.N.C. Email Hacker a Person or a Russian Front? Experts Aren’t Sure.” *The New York Times*, July 27, 2016. http://www.nytimes.com/2016/07/28/us/politics/is-dnc-email-hacker-a-person-or-a-russian-front-experts-arent-sure.html.
Perlroth, Nicole, Mark Scott, and Sheera Frenkel. “Cyberattack Hits Ukraine Then Spreads Internationally.” *The New York Times*, June 27, 2017, sec. Technology. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.
Raiu, Costin, Daniel Moore, Juan Andres Guerrero-Saade, and Thomas Rid. “Penquin’s Moonlit Maze.” *Securelist* (blog), April 3, 2017. https://securelist.com/penquins-moonlit-maze/77883/.
Ranger, Steve. “NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict.” *ZDNet*, June 30, 2014. http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.
Rempfer, Kyle. “DARPA Hopes to Swarm Drones out of C-130s in 2019 Test.” *Air Force Times*, December 19, 2017. https://www.airforcetimes.com/newsletters/daily-news-roundup/2017/12/18/darpa-hopes-to-swarm-drones-out-of-c-130s-in-2019-test/.
Reuters. “China Demands Halt of U.S. Arms Sales to Taiwan.” *Reuters*, April 9, 2018. https://www.reuters.com/article/us-taiwan-usa-submarines/china-demands-halt-of-u-s-arms-sales-to-taiwan-idUSKBN1HG1QJ.
Rid, Thomas. “All Signs Point to Russia Being Behind the DNC Hack.” *Motherboard*, July 25, 2016. http://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack.

Risen, James. “U.S. Secretly Negotiated With Russians to Buy Stolen NSA Documents — and the Russians Offered Trump-Related Material, Too.” *The Intercept* (blog), February 9, 2018. https://theintercept.com/2018/02/09/donald-trump-russia-election-nsa/.

Rivner, Uri. “Anatomy of an Attack.” *Speaking of Security - The RSA Blog* (blog), April 1, 2011. https://blogs.rsa.com/anatomy-of-an-attack/.

Robb, Drew. “Building the Global Heatmap.” *Strava Engineering* (blog), November 1, 2017. https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de.

Rosenbach, Marcel, Hilmar Schmundt, and Christian Stöcker. “Source Code Similarities: Experts Unmask ‘Regin’ Trojan as NSA Tool.” *Spiegel Online*, January 27, 2015, sec. International. http://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html.

Rosenberg, Jay. “2018 Winter Cyber Olympics: Code Similarities with Cyber Attacks in Pyeongchang.” *Intezer* (blog), February 12, 2018. https://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/.

Samit, Sarkar. “Massive DDoS Attack Affecting PSN, Some Xbox Live Apps.” *Polygon*, October 21, 2016. https://www.polygon.com/2016/10/21/13361014/psn-xbox-live-down-ddos-attack-dyn.

Sanchez, Raf. “Russia Uses Missiles and Cyber Warfare to Fight off ‘swarm of Drones’ Attacking Military Bases in Syria.” *The Telegraph*, January 9, 2018. https://www.telegraph.co.uk/news/2018/01/09/russia-fought-swarm-drones-attacking-military-bases-syria/.

Sanger, David E. “Obama Ordered Wave of Cyberattacks Against Iran.” *The New York Times*, June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

———. “U.S. Cyberattacks Target ISIS in a New Line of Combat.” *The New York Times*, April 24, 2016. http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

Sanger, David E., and William J. Broad. “Trump Inherits a Secret Cyberwar Against North Korean Missiles.” *The New York Times*, January 20, 2018, sec. World. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

Sanger, David E., and Mark Mazzetti. “Analysts Find Israel Struck a Syrian Nuclear Project.” *The New York Times*, October 14, 2007. http://www.nytimes.com/2007/10/14/washington/14weapons.html?_r=0.

———. “U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict.” *The New York Times*, February 16, 2016, sec. World. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Sanger, David E., and Eric Schmitt. “Russian Ships Near Data Cables Are Too Close for U.S. Comfort.” *The New York Times*, October 25, 2015, sec. Europe. https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

Schaefer, Ben. “The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism.” *Georgetown Security Studies Review* (blog), March 11, 2018. http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

Schwarz, Matthew J. “Lockheed Martin Suffers Massive Cyberattack.” *Dark Reading* (blog), May 30, 2011. http://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013?

Shane, Scott. “Ex-N.S.A. Worker Accused of Stealing Trove of Secrets Offers to Plead Guilty.” *The New York Times*, January 1, 2018, sec. U.S. https://www.nytimes.com/2018/01/03/us/politics/harold-martin-nsa-guilty-plea-offer.html.

Toonk, Andre. “Chinese ISP Hijacks the Internet.” *BGPMon* (blog), April 8, 2010. https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/.

Volz, Dustin, and Karen Friefeld. “U.S. Issues First Government Guide on Responding to Cyber Attacks,” July 26, 2016. https://www.yahoo.com/tech/u-financial-sanctions-response-cyber-attacks-124106828.html.

Volz, Duston, and Jim Finkle. “U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam.” *Reuters*, March 25, 2016. http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF.

Zetter, Kim. “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.” *WIRED*, July 11, 2011. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Government Publications, Technical Manuals, and Others

Air Land Sea Application Center. “TADIL J: Introduction to Tactical Digital Information Link J and Quick Reference Guide,” June 2000.

Army Headquarters. “US Army Field Manual 3-13 - Information Operations,” November 2003.

Berman, Ilan. The Iranian Cyber Threat, Revisited, § US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (2013). http://www.china.usc.edu/sites/default/files/legacy/AppImages/house-2013-berman-cyber-threats.pdf.

Borland, John. “Analyzing the Internet Collapse.” MIT Technology Review. Accessed January 27, 2018. https://www.technologyreview.com/s/409491/analyzing-the-internet-collapse/.

Boyd, John. “The Essence of Winning and Losing.” June 28, 1995. http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf.

Brady, James S. “Remarks by the President to the White House Press Corps.” The White House, August 20, 2012. https://www.whitehouse.gov/the-press-office/2012/08/20/remarks-president-white-house-press-corps.

Cardon, Edward, Daniel J. O’Donohue, Michael S. Rogers, Jan E. Tighe, and Burke E. Wilson. Cyber Operations: Improving the Military Cybersecurity Posture in an Uncertain Threat Environment, § Committee on Armed Services House of Representatives (n.d.).

CERT.org. “CPU Hardware Vulnerable to Side-Channel Attacks.” Carnegie Mellon University CERT, January 3, 2018. https://www.kb.cert.org/vuls/id/584653.

Chairman of the Joint Chiefs of Staff. “Memorandum of Policy No. 30: Command and Control Warfare,” March 8, 1993.

Charette, Robert N. “This Car Runs on Code.” IEEE Spectrum: Technology, Engineering, and Science News, February 1, 2009. https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code.

Clapper Jr, James R., Michael S. Rogers, and Marcel Lettre. Statement on Foreign Cyber Threats to the United States, § Senate Armed Services Committee (2017).

Coile, Gregory. “WIN-T SATCOM Overview Briefing.” Program Executive Office Command Control Communications-Tactical, 2009.

Comey, James B. “Addressing the Cyber Security Threat.” Speech. Federal Bureau of Investigation, January 7, 2015. https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

Crail, Peter. “IAEA Sends Syria Nuclear Case to UN.” Arms Control Association, July 7, 2011. https://www.armscontrol.org/act/2011_%2007-08/%20IAEA_Sends_Syria_Nuclear_Case_to_UN.

Crawford, Bruce T., James J. Mingus, and Gary P. Martin. The United States Army Network Modernization Strategy, § Committee on the Armed Services (2017). http://docs.house.gov/meetings/AS/AS25/20170927/106451/HHRG-115-AS25-Wstate-CrawfordB-20170927.pdf.

“Cyber Kill Chain.” Lockheed Martin. Accessed June 4, 2017. http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html.

DHS Press Office. “Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security.” Department of Homeland Security, October 7, 2016. https://www.dhs.gov/node/23199.

Epperson, Lynn. “Satellite Communications Within the Army’s WIN-T Architecture.” Program Executive Office Command Control Communications-Tactical, February 6, 2014.

Fleming, Jeremy. “GCHQ Director’s Speech at CYBERUK 2018.” CYBERUK, April 12, 2018.

GCHQ. “Full-Spectrum Cyber Effects.” GCHQ, 2012.

Gettle, Mitch. “Air Force Releases New Mission Statement.” United States Air Force, December 8, 2005. http://www.af.mil/News/ArticleDisplay/tabid/223/Article/132526/air-force-releases-new-mission-statement.aspx.

Global Security. “AEGIS Combat System.” Global Security. Accessed October 2, 2015. http://www.globalsecurity.org/military/systems/ship/systems/aegis.htm.

Government of Georgia. “Russian Cyberwar on Georgia,” November 10, 2008.

Harris, Eimi. “NATO Adds Cyber to Operational Domain.” NATO Association of Canada, July 4, 2016. http://natoassociation.ca/nato-adds-cyber-to-operational-domain/.
Incapsula. “NTP Amplification: DDoS Attack.” Incapsula. Accessed October 2, 2015. https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html.
Israeli Navy. “מלחמת יום הכיפורים - 1973. אתר חיל הים”. Accessed January 23, 2017. http://www.navy.idf.il/1274-he/Navy.aspx.
Johnson, Troy. “Navy Cyber Resilience.” Navy Cybersecurity Division, June 6, 2016.
Kania, Elsa. “Swarms at War: Chinese Advances in Swarm Intelligence.” Jamestown, July 6, 2017. https://jamestown.org/program/swarms-war-chinese-advances-swarm-intelligence/.
Keller, John. “Navy and Air Force Choose DRFM Jammers from Mercury Systems to Help Spoof Enemy Radar.” Military & Aerospace Electronics, June 18, 2014. https://www.militaryaerospace.com/articles/2014/06/mercury-drfm-jammer.html.
Kimmons, Sean. “Cyber Teams Throw Virtual Effects, Defend Networks against ISIS.” United States Army, February 15, 2017. http://www.army.mil/article/182400/cyber_teams_throw_virtual_effects_defend_networks_against_isil.
Lee, Robert M. “Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered.” SANS Industrial Control Systems Security Blog, January 1, 2016. https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered.
Lockheed Martin. “Autonomic Logistics Information System (ALIS).” Lockheed Martin, November 2009. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/alis/CS00086-55%20(ALIS%20Product%20Card).pdf.
———. “Lockheed Martin to Enhance U.S. Navy’s C4ISR Capabilities.” Naval Today, July 1, 2014. http://navaltoday.com/2014/07/01/lockheed-martin-to-enhance-u-s-navys-c4isr-capabilities/.
Malone, Jeff. “Intelligence Support Requirements for Offensive CNO.” presented at the Cyber Warfare and Nation States Conference, Canberra, Australia, August 23, 2010.
McHale, John. “Record Number of Cyber Attacks Hit Lockheed Martin in 2014.” Military Embedded Systems, February 18, 2015. http://mil-embedded.com/3499-record-number-of-cyber-attacks-hit-lockheed-martin-in-2014/.
Microsoft. “Microsoft Security Bulletin MS17-010 - Critical.” Microsoft, July 14, 2017. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.
Ministry of Defense of the Russian Federation. “Head of the Russian General Staff’s Office for UAV Development Major General Alexander Novikov Holds Briefing for Domestic and Foreign Reporters : Ministry of Defence of the Russian Federation.” Ministry of Defense, January 11, 2018. http://eng.mil.ru/en/news_page/country/more.htm?id=12157872@egNews.
MITRE. “MITRE ATT&CK,” 2018. https://attack.mitre.org/wiki/Main_Page.
National Audit Office. “Investigation: WannaCry Cyber Attack and the NHS.” National Audit Office. Accessed January 1, 2018. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.
NAVIOCOM Maryland. “NIOC Maryland Advanced Computer Network Operations Course.” n.d.
NCSC. “Russian Military ‘Almost Certainly’ Responsible for Destructive 2017 Cyber Attack.” UK National Cyber Security Centre, February 15, 2018. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.
NIST. “NVD - CVSS Severity Distribution Over Time.” NIST, 2017. https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time.
NSA. “ANT Product Catalog,” 2009.
———. “Case Studies of Integrated Cyber Operation Techniques.” 2011.
———. “Computer Network Operations - GENIE,” 2013. https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf.
———. “Getting Close to the Adversary: Forward-Based Defense with QFIRE.” June 3, 2011.
———. “SID and DIA Collaborate Virtually on Russian Targets.” National Security Agency, May 18, 2004.
NSA, and USSTRATCOM. “National Initiative Protection Program - Sentry Eagle,” November 23, 2004.
“Operation Aurora.” MuckRock, July 3, 2014. https://www.muckrock.com/foi/united-states-of-america-10/operation-aurora-11765/#files.

People's Liberation Army. "顺应军事变革潮流把握改革主动 - 中国军网-军报记者," January 5, 2016. http://jz.chinamil.com.cn/n2014/tp/content_6843416.htm.
Petkova, Vanja. "Gen. Djurov's Report on the Participation of Bulgarian Troops in the Warsaw Pact Operation in Czechoslovakia, 30 September 1968." Wilson Center, September 30, 1968. Fond 1-B, Record 49, File 158. History and Public Policy Program Digital Archive, Central State Archive. http://digitalarchive.wilsoncenter.org/document/110014.
Poling, Gregory. "New Imagery Release." Asia Maritime Transparency Initiative, September 10, 2015. http://amti.csis.org/new-imagery-release/.
Pomerleau, Mark. "Here's How the Army Wants to Integrate Cyber, EW into Operational Formations." Fifth Domain, October 2, 2017. http://www.fifthdomain.com/dod/army/2017/10/02/heres-how-the-army-wants-to-integrate-cyber-ew-into-operational-formations/.
———. "US Is 'Outgunned' in Electronic Warfare, Says Cyber Commander." C4ISRNET, August 10, 2017. https://www.c4isrnet.com/show-reporter/technet-augusta/2017/08/10/us-is-outgunned-in-electronic-warfare-says-cyber-commander/.
PR Newswire. "Lockheed Martin and DRS Technologies Deliver 4000th AN/UYQ-70 Ship Display System to the U.S. Navy." PR Newswire, May 11, 2012. http://www.prnewswire.com/news-releases/lockheed-martin-and-drs-technologies-deliver-4000th-anuyq-70-ship-display-system-to-the-us-navy-75230862.html.
Prince, Matthew. "Deep Inside a DNS Amplification DDoS Attack." CloudFlare, October 30, 2012. https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/.
Russian Federation. "The Military Doctrine of the Russian Federation," December 25, 2014. http://rusemb.org.uk/press/2029.
Security Service of Ukraine. "Russian Hackers Plan Energy Subversion in Ukraine." Ukrinform, December 28, 2015. http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html.
Shen, Wade. "The Information Domain and the Future of Conflict." presented at the CyCon - International Conference on Cyber Conflict, Tallinn, Estonia, June 1, 2017.
Shields, Nathan P. United States of America V. Park Jin Hyok, No. MJ 18-1479 (United States District Court June 8, 2018).
Symantec. "Petya Ransomware Outbreak: Here's What You Need to Know," October 24, 2017. https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper.
———. "What You Need to Know about the WannaCry Ransomware." Symantec, October 23, 2017. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.
Taiwan Affairs Office of the State Council. "国台办新闻发布会辑录（2018-05-16） 中共中央台湾工作办公室、国务院台湾事务办公室," May 16, 2018. http://www.gwytb.gov.cn/xwfbh/201805/t20180516_11955430.htm.
The State Council Information Office. China's Military Strategy (2015).
ThreatConnect Research. "Shiny Object? Guccifer 2.0 and the DNC Breach." ThreatConnect, June 29, 2016. https://www.threatconnect.com/blog/guccifer-2-0-dnc-breach/.
Todorov, Kenneth, Archer Macy, Richard Formica, Joseph Horn, and Thomas Karako. Panel on Full Spectrum Missile Defense. CSIS, December 4, 2015.
TRADOC. "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040." U.S. Army Training and Doctrine Command, October 2017.
———. "The Operational Environment and the Changing Character of Future Warfare." U.S. Army Training and Doctrine Command, May 31, 2017.
UK Cabinet Office, and Cabinet Office. The UK Cyber Security Strategy: Report on Progress and Forward Plans (2014).
UK Foreign Ministry. "Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks." GOV.UK, December 19, 2017. https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.
UK Ministry of Defense. "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities." UK MoD, February 2018.
Ukraine Ministry of Defense. "Інформація Про 'Втрати у ЗС України 80% Гаубиць Д-30' Не Відповідає Дійсності," January 6, 2017. http://www.mil.gov.ua/news/2017/01/06/informacziya-po-vtrati-u-zs-ukraini-80-gaubicz-d-30%E2%80%9D-ne-vidpovidae-dijsnosti/.
United States Government. "Presidential Policy Directive 20 - U.S. Cyber Operations Policy," October 2012.

United States Industrial Control Systems Cyber Emergency Response Team. “Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT.” ICS-CERT, February 25, 2016. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.
U.S. 24th Air Force. “Commander’s Strategic Vision.” US Air Force, March 8, 2017.
U.S. Air Force. “Air Force Doctrine Document 3-12,” July 15, 2010.
———. “Air Force Policy Directive 17-2: Cyberspace Operations,” April 12, 2016.
U.S. Army. “Army Field Manual 3-12: Cyberspace and Electronic Warfare Operations.” US Army, April 2017.
———. “Army Field Manual 3-38 - Cyber Electromagnetic Activities,” February 12, 2014.
———. “Army Regulation 525-20: Command & Control Countermeasures (C2CM).” U.S. Army Headquarters, July 31, 1992.
———. “Deployed Tactical Network Guidance.” U.S. Army Chief Information Office, May 31, 2012.
———. “U.S. Army Field Manual 100-2-1: Soviet Forces.” Headquarters of the Department of the U.S. Army, July 16, 1984.
———. “U.S. Army Field Manual 100-6: Information Operations.” Headquarters of the Department of the U.S. Army, August 1996.
U.S. Army Headquarters. “Army Doctrine Publication 3-0: Operations.” U.S. Army Headquarters, October 2011.
U.S. Cyber Command. “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” March 23, 2018.
U.S. Department of Defense. “Chinese Exfiltrate Sensitive Military Technology,” 2011. http://www.spiegel.de/media/media-35687.pdf.
———. “Cybercom to Elevate to Combatant Command.” Accessed June 10, 2018. https://www.defense.gov/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/.
———. “Declaratory Policy, Concept of Operations, and Employment Guidelines for Left-of-Launch Capability,” May 10, 2017.
———. “Information Operations Roadmap.” U.S. Department of Defense, October 30, 2003.
———. The Department of Defense Cyber Strategy (2015).
———. “U.S. Department of Defense Directive 3600.01 - Information Operations.” U.S. Department of Defense, December 1996.
———. “U.S. Department of Defense Directive 3600.01 - Information Warfare,” November 1992.
U.S., DNI. “Cyber Threat Framework Lexicon.” Office of the Director of National Intelligence, 2013.
U.S. Homeland Security. “Blueprint for a Secure Cyber Future.” U.S. Homeland Security, November 2011.
U.S. Joint Chiefs of Staff. “Joint Publication 1-02: DoD Dictionary.” U.S. Department of Defense, May 2017.
———. “Joint Publication 2-0: Joint Intelligence.” U.S. Department of Defense, October 22, 2013.
———. “Joint Publication 3-0: Operations,” August 11, 2011.
———. “Joint Publication 3-12: Cyberspace Operations,” May 2, 2013.
———. “Joint Publication 3-12: Cyberspace Operations,” June 8, 2018.
———. “Joint Publication 3-13: Command and Control Warfare (C2W).” U.S. Joint Chief of Staff, February 7, 1996.
———. “Joint Publication 3-13: Information Operations,” November 20, 2014.
———. “Joint Publication 3-13.1: Electronic Warfare,” February 8, 2012.
———. “Joint Publication 5-0: Joint Planning.” US Joint Chief of Staff, June 16, 2017.
U.S. Navy. “The US Navy Fact File: Tomahawk Cruise Missile.” US Navy Official Website. Accessed October 1, 2015. http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1300&ct=2.
U.S. OPM. “Cybersecurity Resource Center.” U.S. Office of Personnel Management. Accessed September 2, 2016. https://www.opm.gov/cybersecurity/.
U.S. Press Secretary. “Statement from the Press Secretary.” The White House, February 15, 2018. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.
U.S. Strategic Command. “U.S. Cyber Command (USCYBERCOM).” U.S. Strategic Command, September 30, 2016. http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.
US-CERT. “Petya Ransomware.” US-CERT, February 15, 2018. https://www.us-cert.gov/ncas/alerts/TA17-181A.
USSR Exercise Control Staff. “Task for the Operational Command Staff Exercise Soyuz-75 for the 4th Army.” Cold War International History Project, March 1975. Polish Institute of National Remembrance. http://digitalarchive.wilsoncenter.org/document/113511.

———. “The Operational-Tactical Exercise of Allied Fleets in the Baltic Sea, Codenamed VAL-77.” Cold War International History Project, 1977. http://digitalarchive.wilsoncenter.org/document/114599.
ViaSat. “Link-16 Message Card,” October 2012. https://www.viasat.com/files/assets/assets/Link16_NPG_Message_Card_100112a.pdf.
White House. “International Strategy for Cyberspace,” May 6, 2011.
Wikileaks. “Vault 7: CIA Hacking Tools Revealed.” Wikileaks, March 7, 2017. https://wikileaks.org/ciav7p1/.
Wong, Edward, Jane Perlez, and Chris Buckley. “China Announces Cuts of 300,000 Troops at Military Parade Showing Its Might.” The New York Times, February 3, 2015. http://www.nytimes.com/2015/09/03/world/asia/beijing-turns-into-ghost-town-as-it-gears-up-for-military-parade.html.
Work, Robert. “Remarks by Deputy Secretary Work on Third Offset Strategy.” U.S. Department of Defense, April 28, 2016. https://www.defense.gov/News/Speeches/Speech-View/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/.